vCloud Director Administratorhandbuch

vCloud Director 1.5.0

Dieses Dokument unterstützt die aufgeführten Produktversionen sowie alle folgenden Versionen, bis das Dokument durch eine neue Auflage ersetzt wird. Die neuesten Versionen dieses Dokuments finden Sie unter http://www.vmware.com/de/support/pubs.

DE-000636-00

vmware®

Die neueste technische Dokumentation finden Sie auf der VMware-Website unter:

http://www.vmware.com/de/support/pubs/

Auf der VMware-Website finden Sie auch die aktuellen Produkt-Updates.

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie Ihre Kommentare und Vorschläge an:

docfeedback@vmware.com

Copyright © 2010, 2011 VMware, Inc. Alle Rechte vorbehalten. Dieses Produkt ist durch Urheberrechtsgesetze, internationale Verträge und mindestens eines der unter http://www.vmware.com/go/patents-de aufgeführten Patente geschützt.

VMware ist eine eingetragene Marke oder Marke der VMware, Inc. in den USA und/oder anderen Ländern. Alle anderen in diesem Dokument erwähnten Bezeichnungen und Namen sind unter Umständen markenrechtlich geschützt.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Global, Inc.
Zweigniederlassung Deutschland
Freisinger Str. 3
85716 Unterschleißheim/Lohhof
Germany
Tel.: +49 (0) 89 3706 17000
Fax: +49 (0) 89 3706 17333
www.vmware.com/de

Inhalt

vCloud Director-Administratorhandbuch 7

1 Erste Schritte mit vCloud Director 9
- Übersicht über die Verwaltung von vCloud Director 9
- Anmelden bei der Webkonsole 12
- Vorbereiten des Systems 12
- Erstellen eines Microsoft Sysprep-Pakets zur Bereitstellung 12
- Ersetzen eines Microsoft Sysprep-Pakets zur Bereitstellung 13
- Festlegen der Benutzereinstellungen 14
- Ändern eines Systemadministratorkennworts 14

2 Hinzufügen von Ressourcen zu vCloud Director 15
- Hinzufügen von vSphere-Ressourcen 15
- Hinzufügen von Cloud-Ressourcen 17

3 Erstellen und Bereitstellen von Organisationen 23
- Grundlagen zu Leases 23
- Erstellen einer Organisation 24
- Zuweisen von Ressourcen zu einer Organisation 28
- Hinzufügen von Netzwerken zu einer Organisation 33

4 Erstellen eines veröffentlichten Katalogs 37
- Aktivieren der Katalogveröffentlichung 37
- Erstellen eines veröffentlichten Katalogs 38
- Hochladen einer vApp-Vorlage 38
- Importieren einer vApp-Vorlage aus vSphere 39
- Hochladen einer Mediendatei 39
- Importieren einer Mediendatei aus vSphere 40
- Katalog veröffentlichen 40

5 Verwalten von Cloud-Ressourcen 43
- Verwalten von Provider-vDCs 43
- Verwalten von Organisations-vDCs 48
- Verwalten externer Netzwerke 55
- Verwalten von Organisationsnetzwerken 56
- Verwalten von Netzwerkpools 75
- Verwalten von Cloud-Zellen 77

6 Verwalten von vSphere-Ressourcen 79
- Verwalten von vSphere vCenter Server 79
- Verwalten von vSphere ESX/ESXi-Hosts 81

Verwalten von vSphere-Datenspeichern 83
Verwalten freigelegter Objekte 84

7 Verwalten von Organisationen 87
Aktivieren oder Deaktivieren einer Organisation 87
Löschen einer Organisation 88
Bearbeiten des Organisationsnamens 88
Bearbeiten des vollständigen Namens und der Beschreibung einer Organisation 88
Bearbeiten der LDAP-Optionen für die Organisation 89
Bearbeiten der Richtlinien zur Veröffentlichung von Katalogen für die Organisation 90
Bearbeiten der E-Mail-Einstellungen für eine Organisation 90
Bearbeiten von Lease-, Kontingent- und Grenzwerteinstellungen auf Organisationsebene 91
Hinzufügen eines Katalogs zu einer Organisation 92
Verwalten von Organisationsressourcen 92
Verwalten der Benutzer und Gruppen von Organisationen 92
Verwalten von Organisations-vApps und virtuellen Maschinen 93

8 Verwalten von Systemadministratoren und Rollen 97
Hinzufügen eines Systemadministrators 97
Importieren eines Systemadministrators 98
Aktivieren oder Deaktivieren eines Systemadministrators 98
Löschen eines Systemadministrators 98
Bearbeiten des Profils und der Kontaktinformationen des Systemadministrators 98
Versenden einer E-Mail-Benachrichtigung an Benutzer 99
Löschen eines Systemadministrators, der nicht mehr auf das System zugreifen kann 99
Importieren einer LDAP-Gruppe 99
Löschen einer LDAP-Gruppe 100
Ändern einer LDAP-Gruppenbeschreibung 100
Rollen und Rechte 100
Erstellen einer Rolle 101
Kopieren einer Rolle 101
Bearbeiten einer Rolle 101
Löschen einer Rolle 101

9 Verwalten der Systemeinstellungen 103
Bearbeiten der allgemeinen Systemeinstellungen 103
Allgemeine Systemeinstellungen 104
Konfigurieren der SMTP-Einstellungen 105
Konfigurieren der Systembenachrichtigungseinstellungen 106
Konfigurieren von blockierenden Aufgaben und Benachrichtigungen 106
Konfigurieren der System-LDAP-Einstellungen 108
Anpassen der Benutzeroberfläche des vCloud Director-Clients 111
Konfigurieren der öffentlichen Web-URL 113
Konfigurieren der Proxy-Adresse der öffentlichen Konsole 113
Konfigurieren der Basis-URL für die öffentliche REST API 113
Konfigurieren der Kontosperrungsrichtlinie 114

10 Überwachen von vCloud Director 115
Anzeigen von Aufgaben und Ereignissen 115
Überwachen und Verwalten von blockierenden Aufgaben 117
Anzeigen von Informationen zur Nutzung bzw. Auslastung eines Provider-vDCs 118
Anzeigen von Informationen zur Nutzung bzw. Auslastung eines Organisations-vDCs 118
Verwenden des vCloud Director-JMX-Dienstes 118
Anzeigen der vCloud Director-Protokolle 119
vCloud Director und Kostenberichte 119
Überwachen von Dateien unter Quarantäne 120

11 Rollen und Rechte 123
Vordefinierte Rollen und ihre Rechte 123

Index 127

vCloud Director-Administratorhandbuch

Das *VMware vCloud Director-Administratorhandbuch* enthält Informationen für den vCloud Director-Systemadministrator zum Hinzufügen von Ressourcen zum System, zum Erstellen und Bereitstellen von Organisationen, zum Verwalten von Ressourcen und Organisationen und zum Überwachen des Systems.

Zielgruppe

Dieses Handbuch wendet sich an alle Benutzer, die eine vCloud Director-Installation konfigurieren und verwalten möchten. Die in ihm enthaltenen Informationen wurden für erfahrene Systemadministratoren erstellt, die mit Linux, Windows, IP-Netzwerken und VMware vSphere vertraut sind.

Erste Schritte mit vCloud Director 1

Wenn Sie sich das erste Mal bei der vCloud Director-Webkonsole anmelden, werden Sie auf der Registerkarte **[Startseite]** durch die benötigten Schritte zur Konfiguration der Installation geleitet.

Sie können auch Ihre Benutzereinstellungen konfigurieren und ein Microsoft Sysprep-Bereitstellungspaket erstellen, um eine Gast-Anpassung in virtuellen Maschinen unter vCloud Director zu unterstützen.

Dieses Kapitel behandelt die folgenden Themen:

- „Übersicht über die Verwaltung von vCloud Director“, auf Seite 9
- „Anmelden bei der Webkonsole“, auf Seite 12
- „Vorbereiten des Systems“, auf Seite 12
- „Erstellen eines Microsoft Sysprep-Pakets zur Bereitstellung“, auf Seite 12
- „Ersetzen eines Microsoft Sysprep-Pakets zur Bereitstellung“, auf Seite 13
- „Festlegen der Benutzereinstellungen“, auf Seite 14
- „Ändern eines Systemadministratorkennworts“, auf Seite 14

Übersicht über die Verwaltung von vCloud Director

VMware vCloud Director ist eine Softwareanwendung, die Funktionen zum Erstellen von sicheren Clouds für mehrere Mandanten bereitstellt. Zu diesem Zweck bündelt sie virtuelle Infrastrukturressourcen zu virtuellen Datencentern, die den Benutzern über webbasierte Portale und Programmierschnittstellen als vollständig automatisierter, katalogbasierter Dienst bereitgestellt werden.

Das *VMware vCloud Director-Administratorhandbuch* enthält Informationen zum Hinzufügen von Ressourcen zum System, zum Erstellen und Bereitstellen von Organisationen, zum Verwalten von Ressourcen und Organisationen und zum Überwachen des Systems.

vSphere-Ressourcen

vCloud Director stellt Prozessorleistung und Arbeitsspeicher für den Betrieb virtueller Maschinen auf der Grundlage von vSphere-Ressourcen bereit. Außerdem bieten vSphere-Datenspeicher Speicher für Dateien virtueller Maschinen und andere Dateien, die für den Betrieb virtueller Maschinen erforderlich sind. vCloud Director verwendet auch vSphere Distributed Switches und vSphere-Portgruppen, um Netzwerke virtueller Maschinen zu unterstützen.

Sie können die zugrunde liegenden vSphere-Ressourcen zur Erstellung von Cloud-Ressourcen verwenden.

Cloud-Ressourcen

Cloud-Ressourcen sind eine Abstraktion der zugrunde liegenden vSphere-Ressourcen. Sie stellen die Rechen- und Arbeitsspeicherressourcen für virtuelle Maschinen und vApps unter vCloud Director bereit. Eine vApp ist ein virtuelles System, das eine oder mehrere virtuelle Maschinen sowie Parameter zur Festlegung von Betriebsdetails enthält. Cloud-Ressourcen bieten auch Zugriff auf Speicher und Netzwerkkonnektivität.

Cloud-Ressourcen sind u. a. virtuelle Datencenter in Form von Provider- und Organisations-vDCs, externe Netzwerke, Organisationsnetzwerke und Netzwerkpools. Bevor Sie Cloud-Ressourcen zu vCloud Director hinzufügen können, müssen Sie vSphere-Ressourcen hinzufügen.

Virtuelle Provider-Datencenter

Virtuelle Provider-Datencenter (Provider-vDC) kombinieren die Rechen- und Arbeitsspeicherressourcen von einem einzelnen vCenter Server-Ressourcenpool mit den Speicherressourcen von einem oder mehreren Datenspeichern, die für diesen Ressourcenpool zur Verfügung stehen.

Sie können mehrere Provider-vDCs für Benutzer an unterschiedlichen geografischen Standorten oder aus verschiedenen Geschäftseinheiten oder auch für Benutzer mit unterschiedlichen Systemleistungsanforderungen erstellen.

Virtuelle Organisations-Datencenter

Virtuelle Organisations-Datencenter (Organisations-vDCs) stellen Ressourcen für Organisationen bereit. Sie werden von einem Provider-vDC abgetrennt. Organisations-vDCs stellen eine Umgebung bereit, in der virtuelle Systeme gespeichert, bereitgestellt und betrieben werden können. Darüber hinaus stellen sie auch Speicher für virtuelle Medien, beispielsweise Disketten und CD-ROMs, bereit.

Eine einzelne Organisation kann über mehrere Organisations-vDCs verfügen.

vCloud Director-Netzwerke

vCloud Director unterstützt drei Arten von Netzwerken.

- Externe Netzwerke
- Organisationsnetzwerke
- vApp-Netzwerke

Einige Organisationsnetzwerke und alle vApp-Netzwerke werden von Netzwerkpools gestützt.

Externe Netzwerke

Bei einem externen Netzwerk handelt es sich um ein logisches, differenziertes Netzwerk auf der Basis einer vSphere-Portgruppe. Organisationsnetzwerke können eine Verbindung zu externen Netzwerken herstellen und auf diese Weise für die virtuellen Maschinen in vApps Internetkonnektivität bereitstellen.

Die Berechtigung zum Erstellen und Verwalten von externen Netzwerken ist Systemadministratoren vorbehalten.

Organisationsnetzwerke

Organisationsnetzwerke sind Bestandteile von vCloud Director-Organisationen. Sie stehen allen vApps in der Organisation zur Verfügung. Organisationsnetzwerke ermöglichen es vApps, Daten innerhalb einer Organisation miteinander auszutauschen. Sie können ein Organisationsnetzwerk mit einem externen Netzwerk verbinden, um externe Konnektivität bereitzustellen. Sie können auch ein isoliertes Organisationsnetzwerk erstellen, dessen Skopus auf die Organisation beschränkt ist. Bestimmte Arten von Organisationsnetzwerken werden von Netzwerkpools gestützt.

Die Berechtigung zum Erstellen von Organisationsnetzwerken ist Systemadministratoren vorbehalten. System- und Organisationsadministratoren verfügen beide über die erforderlichen Berechtigungen, Organisationsnetzwerke zu verwalten; die Berechtigungen von Organisationsadministratoren sind jedoch stärker beschränkt.

vApp-Netzwerke

vApp-Netzwerke sind Bestandteile von vApps und ermöglichen es virtuellen Maschinen in der vApp, Daten miteinander auszutauschen. Sie können ein vApp-Netzwerk mit einem Organisationsnetzwerk verbinden, um für die vApp eine Möglichkeit zu schaffen, Daten mit den anderen vApps in der Organisation und sogar außerhalb der Organisation auszutauschen, falls das Organisationsnetzwerk mit einem externen Netzwerk verbunden ist. vApp-Netzwerke werden von Netzwerkpools gestützt.

Die meisten Benutzer mit Zugriff auf eine vApp können eigene vApp-Netzwerke erstellen und verwalten. Das Arbeiten mit vApp-Netzwerken ist im *VMware vCloud Director-Benutzerhandbuch* beschrieben.

Netzwerkpools

Bei einem Netzwerkpool handelt es sich um eine Gruppe undifferenzierter Netzwerke, die in einem Organisations-vDC zur Verfügung gestellt werden. Ein Netzwerkpool wird von vSphere-Netzwerkressourcen, z. B. VLAN-IDs, Portgruppen oder cloudisolierten Netzwerken, gestützt. vCloud Director verwendet Netzwerkpools, um Organisationsnetzwerke mit NAT-Routing und interne Organisationsnetzwerke sowie alle vApp-Netzwerke zu unterstützen. Der Datenverkehr in den einzelnen Netzwerken wird auf der Ebene von Layer 2 von allen anderen Netzwerken isoliert.

Jedes Organisations-vDC in vCloud Director kann über einen Netzwerkpool verfügen. Mehrere Organisations-vDCs können denselben Netzwerkpool nutzen. Der Netzwerkpool für ein Organisations-vDC stellt die Netzwerke bereit, die erstellt wurden, um das Netzwerkkontingent für ein Organisations-vDC zu erfüllen.

Die Berechtigung zum Erstellen und Verwalten von Netzwerkpools ist Systemadministratoren vorbehalten.

Organisationen

Durch die Verwendung von Organisationen ist vCloud Director mandantenfähig. Eine Organisation ist eine Verwaltungseinheit für eine Sammlung von Benutzern, Gruppen und Rechenressourcen. Benutzer melden sich auf der Ebene von Organisationen mit den Anmeldeinformationen an, die vom Organisationsadministrator beim Erstellen oder Importieren des Benutzers angelegt wurden. Systemadministratoren erstellen Organisationen und stellen sie bereit, während Organisationsadministratoren Benutzer, Gruppen und Kataloge der Organisation verwalten. Die Aufgaben von Organisationsadministratoren sind im *VMware vCloud Director-Benutzerhandbuch* beschrieben.

Benutzer und Gruppen

Organisationen können über eine beliebige Anzahl an Benutzern und Gruppen verfügen. Benutzer können vom Organisationsadministrator erstellt oder aus einem Verzeichnisdienst wie LDAP importiert werden. Gruppen müssen jedoch aus dem Verzeichnisdienst importiert werden. Die Berechtigungen innerhalb einer Organisation werden durch Zuweisung von Rechten und Rollen zu Benutzern und Gruppen gesteuert.

Kataloge

Organisationen verwenden Kataloge, um vApp-Vorlagen und Mediendateien zu speichern. Die Mitglieder einer Organisation, die Zugriff auf einen Katalog haben, können die vApp-Vorlagen und Mediendateien des Katalogs zum Erstellen eigener vApps verwenden. Systemadministratoren können einer Organisation erlauben, Kataloge zu veröffentlichen, um sie auf diese Weise anderen Organisationen zur Verfügung zu stellen. Organisationsadministratoren können auswählen, welche Objekte des Katalogs sie für die Benutzer bereitstellen möchten.

Anmelden bei der Webkonsole

Sie können auf die Benutzeroberfläche von vCloud Director mithilfe eines Webbrowsers zugreifen.

Eine Liste der unterstützten Browser finden Sie im *Installations- und Konfigurationshandbuch zu VMware vCloud Director*.

Voraussetzungen

Sie müssen für diesen Vorgang den Benutzernamen und das Kennwort des Systemadministrators, dessen Konto bei der Einrichtung des Systems erstellt wurde, bereithalten.

Vorgehensweise

1 Öffnen Sie in einem Webbrowser die URL **`https://`*`hostname.domäne.tld`*`/cloud`**.

Ersetzen Sie dabei *hostname.domäne.tld* durch den vollständig qualifizierten Domänennamen für die primäre IP-Adresse des vCloud Director-Serverhosts. Beispiel: **`http://cloud.beispiel.com/cloud`**.

2 Geben Sie den Benutzernamen des Systemadministrators und das zugehörige Kennwort ein und klicken Sie dann auf **[Anmelden]** .

vCloud Director zeigt eine Liste der anschließend durchzuführenden Aufgaben an.

Vorbereiten des Systems

Die Registerkarte **[Startseite]** in der vCloud Director-Webkonsole enthält Links zu den Aufgaben, die zur Vorbereitung des zu verwendenden Systems ausgeführt werden müssen. Die Links sind verfügbar, nachdem die Aufgaben zur Erfüllung der Voraussetzungen ausgeführt wurden.

Weitere Informationen zu den einzelnen Aufgaben erhalten Sie unter Tabelle 1-1.

Tabelle 1-1. Schnellstartaufgaben

Aufgabe	Weitere Informationen
Anfügen eines vCenters	„Anfügen von vCenter Server“, auf Seite 15
Erstellen eines virtuellen Provider-Datencenters	„Erstellen eines virtuellen Provider-Datencenters“, auf Seite 18
Erstellen eines externes Netzwerks	„Hinzufügen eines externen Netzwerks“, auf Seite 19
Erstellen eines Netzwerkpools	„Netzwerkpools“, auf Seite 20
Erstellen einer Organisation	„Erstellen einer Organisation“, auf Seite 24
Zuweisen von Ressourcen zu einer Organisation	„Erstellen eines Organisations-vDC“, auf Seite 48
Hinzufügen eines Netzwerks zu einer Organisation	„Erstellen von Organisationsnetzwerken“, auf Seite 56
Hinzufügen eines Katalogs zu einer Organisation	„Hinzufügen eines Katalogs zu einer Organisation“, auf Seite 92

Erstellen eines Microsoft Sysprep-Pakets zur Bereitstellung

Damit vCloud Director bei bestimmten Windows-Gastbetriebssystemen eine Gast-Anpassung für virtuelle Maschinen durchführen kann, müssen Sie für alle Cloud-Zellen in der Installation ein Microsoft Sysprep-Paket zur Bereitstellung erstellen.

vCloud Director speichert bei der Installation einige Dateien im Ordner `sysprep` des vCloud Director-Serverhosts. Achten Sie darauf, diese Dateien nicht zu überschreiben, wenn Sie das Sysprep-Paket erstellen.

Voraussetzungen

Zugriff auf die Sysprep-Binärdateien für Windows 2000, Windows 2003 (32- und 64-Bit) und Windows XP (32- und 64-Bit)

Vorgehensweise

1 Kopieren Sie die Sysprep-Binärdateien für die einzelnen Betriebssysteme an einen geeigneten Speicherort auf dem vCloud Director-Serverhost.

Es wird für jedes Betriebssystem ein eigener Ordner benötigt.

HINWEIS Bei den Ordnernamen wird die Groß-/Kleinschreibung berücksichtigt.

Gast-BS	Kopierziel
Windows 2000	*SysprepBinariesDirectory* `/win2000`
Windows 2003 (32-Bit)	*SysprepBinariesDirectory* `/win2k3`
Windows 2003 (64-Bit)	*SysprepBinariesDirectory* `/win2k3_64`
Windows XP (32-Bit)	*SysprepBinariesDirectory* `/winxp`
Windows XP (64-Bit)	*SysprepBinariesDirectory* `/winxp_64`

SysprepBinariesDirectory ist der Speicherort, den Sie als Ziel für die kopierten Binärdateien festgelegt haben.

2 Führen Sie den Befehl `/opt/vmware/cloud-director/deploymentPackageCreator/createSysprepPackage.sh` *SysprepBinariesDirectory* aus.

Beispiel: `/opt/vmware/cloud-director/deploymentPackageCreator/createSysprepPackage.sh /root/MeineSysprepdateien`.

3 Verwenden Sie den Befehl `service vmware-vcd restart`, um die Cloud-Zelle neu zu starten.

4 Wenn Sie über mehrere Cloud-Zellen verfügen, kopieren Sie die Paket- und die Eigenschaftsdatei in alle Cloud-Zellen.

```
scp /opt/vmware/cloud-director/guestcustomization/vcloud_sysprep.properties
/opt/vmware/cloud-director/guestcustomization/windows_deployment_package_sysprep.cab
root@next_cell_IP:/opt/vmware/cloud-director/guestcustomization
```

5 Starten Sie die Cloud-Zellen, in die Sie die Dateien kopiert haben, neu.

Ersetzen eines Microsoft Sysprep-Pakets zur Bereitstellung

Wenn Sie bereits ein Microsoft Sysprep-Paket zur Bereitstellung erstellt haben und ein neues generieren möchten, müssen Sie jeweils das Sysprep-Paket in den einzelnen Cloud-Zellen in der Installation ersetzen.

Voraussetzungen

Zugriff auf die Sysprep-Binärdateien für Windows 2000, Windows 2003 (32- und 64-Bit) und Windows XP (32- und 64-Bit)

Vorgehensweise

1 Verwenden Sie den Befehl `service vmware-vcd stop`, um die erste Cloud-Zelle anzuhalten.

2 Kopieren Sie die neuen Sysprep-Binärdateien für die einzelnen Betriebssysteme an einen geeigneten Speicherort auf dem vCloud Director-Serverhost.

Es wird für jedes Betriebssystem ein eigener Ordner benötigt.

HINWEIS Bei den Ordnernamen wird die Groß-/Kleinschreibung berücksichtigt.

Gast-BS	Kopierziel
Windows 2000	*SysprepBinariesDirectory* `/win2000`
Windows 2003 (32-Bit)	*SysprepBinariesDirectory* `/win2k3`
Windows 2003 (64-Bit)	*SysprepBinariesDirectory* `/win2k3_64`
Windows XP (32-Bit)	*SysprepBinariesDirectory* `/winxp`
Windows XP (64-Bit)	*SysprepBinariesDirectory* `/winxp_64`

SysprepBinariesDirectory ist der Speicherort, den Sie als Ziel für die kopierten Binärdateien festgelegt haben.

3 Führen Sie den Befehl `/opt/vmware/cloud-director/deploymentPackageCreator/createSysprepPackage.sh` *SysprepBinariesDirectory* aus.

   Beispiel: `/opt/vmware/cloud-director/deploymentPackageCreator/createSysprepPackage.sh /root/MeineSysprepdateien`.

4 Verwenden Sie den Befehl `service vmware-vcd restart`, um die Cloud-Zelle neu zu starten.

5 Wenn Sie über mehrere Cloud-Zellen verfügen, halten Sie sie nacheinander an und kopieren Sie die Paket- und die Eigenschaftsdatei in die Cloud-Zellen.

```
scp /opt/vmware/cloud-director/guestcustomization/vcloud_sysprep.properties
/opt/vmware/cloud-director/guestcustomization/windows_deployment_package_sysprep.cab
root@next_cell_IP:/opt/vmware/cloud-director/guestcustomization
```

6 Starten Sie die Cloud-Zellen, in die Sie die Dateien kopiert haben, neu.

Festlegen der Benutzereinstellungen

Sie können bestimmte Voreinstellungen zur Anzeige und zu Systemwarnungen festlegen, die bei jeder Anmeldung beim System neu geladen werden.

Vorgehensweise

1 Klicken Sie auf der Titelleiste der Webkonsole auf **[Einstellungen]** .

2 Klicken Sie auf die Registerkarte **[Standardeinstellungen]** .

3 Wählen Sie die Seite aus, die beim Anmelden angezeigt werden soll.

4 Wählen Sie durch Angabe der Anzahl an Tagen bzw. Stunden aus, zu welchem Zeitpunkt vor dem Ablauf des Laufzeit-Lease Sie eine E-Mail-Benachrichtigung erhalten möchten.

5 Wählen Sie durch Angabe der Anzahl an Tagen bzw. Stunden aus, zu welchem Zeitpunkt Sie vor dem Ablauf des Speicher-Lease eine E-Mail-Benachrichtigung erhalten möchten.

6 Klicken Sie auf **[OK]** .

Ändern eines Systemadministratorkennworts

Sie können das Kennwort für Ihr Systemadministratorkonto ändern.

Ein Ändern des Kennworts ist ausschließlich für lokale Benutzer (keine LDAP-Benutzer) möglich.

Vorgehensweise

1 Klicken Sie in der Titelleiste der Webkonsole auf **[Einstellungen]** .

2 Klicken Sie auf die Registerkarte **[Kennwort ändern]** .

3 Geben Sie Ihr altes Kennwort und zweimal Ihr neues Kennwort ein und klicken Sie dann auf **[OK]** .

Hinzufügen von Ressourcen zu vCloud Director 2

vCloud Director entnimmt seine Ressourcen der zugrunde liegenden virtuellen Infrastruktur einer vSphere-Installation. Sie registrieren vSphere-Ressourcen in vCloud Director, um sie anschließend Organisationen in der vCloud Director-Installation zur Nutzung zuzuweisen.

Dieses Kapitel behandelt die folgenden Themen:

- „Hinzufügen von vSphere-Ressourcen“, auf Seite 15
- „Hinzufügen von Cloud-Ressourcen“, auf Seite 17

Hinzufügen von vSphere-Ressourcen

vCloud Director stellt Prozessorleistung und Arbeitsspeicher für den Betrieb von virtuellen Maschinen auf der Grundlage von vSphere-Ressourcen bereit. Darüber hinaus stellen vSphere-Datenspeicher Speicherplatz für Dateien von virtuellen Maschinen und andere Dateien, die beim Betrieb der virtuellen Maschinen benötigt werden, zur Verfügung.

Weitere Information zu den Systemanforderungen von vCloud Director und zu den unterstützten Versionen von vCenter Server und ESX/ESXi erhalten Sie im *Installations- und Konfigurationshandbuch zu VMware vCloud Director*.

Anfügen von vCenter Server

Wenn Sie einen vCenter Server anfügen, können Sie seine Ressourcen in vCloud Director verfügbar machen. Nach dem Anfügen von vCenter Server können Sie seine Ressourcenpools, Datenspeicher und Netzwerke einem virtuellen Provider-Datencenter zuordnen.

Voraussetzungen

Es ist eine Instanz von vShield Manager installiert und für vCloud Director konfiguriert. Weitere Informationen erhalten Sie im *Installations- und Konfigurationshandbuch zu VMware vCloud Director*.

Vorgehensweise

1 Öffnen des Assistenten zum Anfügen neuer vCenter Server auf Seite 16

Öffnen Sie den Assistenten zum Anfügen neuer vCenter Server, um den Vorgang zum Anfügen von vCenter Server an vCloud Director zu starten.

2 Bereitstellen von Verbindungs- und Anzeigeinformationen für den vCenter Server auf Seite 16

Um einen vCenter Server an vCloud Director anzufügen, müssen Sie für den vCenter Server die erforderlichen Verbindungsdaten und einen Anzeigenamen bereitstellen.

3 Herstellen der Verbindung zu vShield Manager auf Seite 16

vCloud Director benötigt vShield Manager, um Netzwerkdienste bereitzustellen. Jeder vCenter Server, den Sie an vCloud Director anfügen, benötigt einen eigenen vShield Manager.

4 Bestätigen der Einstellungen und Anfügen von vCenter Server auf Seite 17

Überprüfen Sie die eingegebenen Einstellungen, bevor Sie den neuen vCenter Server anfügen.

Öffnen des Assistenten zum Anfügen neuer vCenter Server

Öffnen Sie den Assistenten zum Anfügen neuer vCenter Server, um den Vorgang zum Anfügen von vCenter Server an vCloud Director zu starten.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie im linken Bereich auf **[vCenter]** .

2 Klicken Sie auf die Schaltfläche **[Neues vCenter anfügen]** .

Der Assistent zum Anfügen neuer vCenter Server wird gestartet.

Bereitstellen von Verbindungs- und Anzeigeinformationen für den vCenter Server

Um einen vCenter Server an vCloud Director anzufügen, müssen Sie für den vCenter Server die erforderlichen Verbindungsdaten und einen Anzeigenamen bereitstellen.

Vorgehensweise

1 Geben Sie den Hostnamen oder die IP-Adresse von vCenter Server ein.

2 Wählen Sie die Portnummer aus, die dieser vCenter Server verwendet.

Die Standardportnummer ist 443.

3 Geben Sie den Benutzernamen und das zugehörige Kennwort eines vCenter Server-Administrators ein.

Dem Benutzerkonto muss in vCenter die Administratorrolle zugeordnet sein.

4 Geben Sie einen Namen für den vCenter Server ein.

Der eingegebene Name wird in vCloud Director als Anzeigename für den vCenter Server verwendet.

5 (Optional) Geben Sie eine Beschreibung für den vCenter Server ein.

6 Klicken Sie auf **[Weiter]** , um die Einstellungen zu speichern und zur nächsten Seite zu gelangen.

Herstellen der Verbindung zu vShield Manager

vCloud Director benötigt vShield Manager, um Netzwerkdienste bereitzustellen. Jeder vCenter Server, den Sie an vCloud Director anfügen, benötigt einen eigenen vShield Manager.

Vorgehensweise

1 Geben Sie den Hostnamen oder die IP-Adresse des vShield Managers ein, der für den angefügten vCenter Server verwendet werden soll.

2 Geben Sie einen Benutzernamen und ein Kennwort für die Verbindung zu dem vShield Manager ein.

Der Standardbenutzername lautet **`admin`** und das Standardkennwort lautet **`default`**. Diese Standardeinstellungen können über die Benutzeroberfläche von vShield Manager geändert werden.

3 Klicken Sie auf **[Weiter]** , um die Einstellungen zu speichern und zur nächsten Seite zu gelangen.

Bestätigen der Einstellungen und Anfügen von vCenter Server

Überprüfen Sie die eingegebenen Einstellungen, bevor Sie den neuen vCenter Server anfügen.

Vorgehensweise

1 Überprüfen Sie die Einstellungen für den vCenter Server und vShield Manager.

2 (Optional) Klicken Sie auf **[Zurück]** , wenn Sie die Einstellungen ändern möchten.

3 Klicken Sie auf **[Fertigstellen]** , um die Einstellungen zu übernehmen und den vCenter Server anzufügen.

vCloud Director fügt den neuen vCenter Server an und registriert seine Ressource für virtuelle Provider-Datencenter.

Weiter

Weisen Sie in dem vCenter Server einen vShield for VMware vCloud Director-Lizenzschlüssel zu.

Zuweisen eines vShield-Lizenzschlüssels in vCenter

Nach dem Anhängen von vCenter Server an vCloud Director müssen Sie anschließend im vSphere Client einen vShield for VMware vCloud Director-Lizenzschlüssel zuweisen.

Voraussetzungen

Der vSphere Client muss mit dem vCenter Server-System verbunden sein.

Vorgehensweise

1 Wählen Sie auf dem vSphere Client-Host, der mit dem vCenter Server-System verbunden ist, den Menübefehl **[Startseite] > [Lizenzierung]** .

2 Wählen Sie die Option **[Ressource]** , um die Berichtansicht anzuzeigen.

3 Klicken Sie mit der rechten Maustaste auf die vShield-Edge-Ressource und wählen Sie den Befehl **[Lizenzschlüssel bearbeiten]** .

4 Wählen Sie die Option **[Neuen Lizenzschlüssel zuweisen]** und klicken Sie dann auf **[Schlüssel eingeben]** .

5 Geben Sie den Lizenzschlüssel ein, geben Sie bei Bedarf eine Beschriftung für den Schlüssel ein und klicken Sie dann auf **[OK]** .

   Sie können den vShield for VMware vCloud Director-Lizenzschlüssel verwenden, den Sie beim Kauf Ihrer Lizenz von vCloud Director erhalten haben. Sie können diesen Lizenzschlüssel auch in mehreren vCenter Server verwenden.

6 Klicken Sie auf **[OK]** .

Hinzufügen von Cloud-Ressourcen

Cloud-Ressourcen stellen eine Abstraktion der zugrunde liegenden vSphere-Ressourcen dar, die die Rechen- und Speicherressourcen für virtuelle Maschinen und vApps unter vCloud Director sowie den Zugriff auf Speicher und die Netzwerkkonnektivität bereitstellen.

Cloud-Ressourcen sind u. a. virtuelle Datencenter in Form von so genannten Provider- und Organisations-vDCs, externe Netzwerke, Organisationsnetzwerke und Netzwerkpools. Sie können vCloud Director erst dann Ressourcen hinzufügen, wenn Sie sie vSphere hinzugefügt haben.

Weitere Informationen zu virtuellen Datencentern in Organisationen erhalten Sie unter „Zuweisen von Ressourcen zu einer Organisation“, auf Seite 28.

Weitere Informationen zu Organisationsnetzwerken erhalten Sie unter „Hinzufügen von Netzwerken zu einer Organisation“, auf Seite 33.

Virtuelle Provider-Datencenter

Virtuelle Provider-Datencenter kombinieren die Rechen- und Arbeitsspeicherressourcen von einem vCenter Server-Ressourcenpool mit den Speicherressourcen von einem oder mehreren Datenspeichern, die mit diesem Ressourcenpool verbunden sind.

Provider-vDCs sind die Quelle für Organisations-vDCs.

Erstellen eines virtuellen Provider-Datencenters

Sie können ein Provider-vDC erstellen, um Rechen-, Arbeitsspeicher- und Speicherressourcen von vSphere in vCloud Director zu registrieren. Sie können mehrere Provider-vDCs für Benutzer an unterschiedlichen geografischen Standorten oder aus verschiedenen Geschäftseinheiten oder auch für Benutzer mit eigenen Systemleistungsanforderungen erstellen.

Provider-vDCs können nur einen einzigen Ressourcenpool aus einem einzigen vCenter Server beinhalten.

Wenn Sie beabsichtigen, einen Ressourcenpool hinzuzufügen, der Teil eines Clusters ist, welcher vSphere HA verwendet, müssen Sie wissen, wie vSphere HA die Slotgröße berechnet. Weitere Informationen zu Slotgrößen und zur Anpassung des Systemverhaltens von vSphere HA erhalten Sie im *VMware vSphere-Verfügbarkeitshandbuch*.

Voraussetzungen

Prüfen Sie, ob mindestens ein vCenter Server mit einem für vCloud Director verfügbaren Ressourcenpool angefügt ist. Der Ressourcenpool muss sich in einem vCenter-Cluster befinden, der für die automatische DRS-Verwendung konfiguriert ist. Der vCenter Server muss den vShield für VMware vCloud Director-Lizenzschlüssel verwenden.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Provider-vDCs]** .

2 Klicken Sie auf **[Neues Provider-vDC]** .

3 Geben Sie einen Namen und bei Bedarf eine Beschreibung ein.

   Über den Namen und die Beschreibung können Sie Hinweise zu vSphere-Funktionen geben, die Provider-vDCs, wie beispielsweise vSphere HA, zur Verfügung gestellt werden.

4 Wählen Sie die letzte unterstützte Hardwareversion aus und klicken Sie dann auf **[Weiter]** .

   Mit dieser Auswahl wird die neueste unterstützte Hardwareversion für virtuelle Maschinen in Organisations-vDCs, die auf diesem Provider-vDC basieren, festgelegt. **[Hardwareversion 8]** benötigt ESX/ESXi 5.0-Hosts. Wenn dieses Provider-vDC einen Ressourcenpool verwendet, der sowohl ESX/ESXi 5.0- als auch ESX/ESXi 4.x-Hosts enthält, wählen Sie **[Hardwareversion 7]** .

5 Wählen Sie einen vCenter Server und einen Ressourcenpool aus und klicken Sie dann auf **[Weiter]** .

   Wenn für den vCenter Server keine Ressourcenpools verfügbar sind, werden keine Ressourcenpools in der Liste angezeigt.

6 Wählen Sie einen oder mehrere Datenspeicher aus, klicken Sie auf **[Hinzufügen]** und klicken Sie auf **[Weiter]** .

vCloud Director unterstützt bei Provider-vDCs nicht die Verwendung von schreibgeschützten Datenspeichern. In der Regel werden schreibgeschützte Datenspeicher nicht in der Liste aufgeführt, aber einige schreibgeschützte NFS-Datenspeicher können angezeigt werden. Fügen Sie diese Datenspeicher dem Provider-vDC nicht hinzu.

Verwenden Sie nur gemeinsam genutzten Speicher, da vSphere DRS die Migration von virtuellen Maschinen im lokalen Speicher nicht unterstützt.

7 Geben Sie den Root-Benutzernamen und das zugehörige Kennwort für die ESX/ESXi-Hosts ein und klicken Sie dann auf **[Weiter]** .

8 Klicken Sie auf **[Fertigstellen]** , um das Provider-vDC zu erstellen.

Externe Netzwerke

Bei einem externen Netzwerk handelt es sich um ein logisches, differenziertes Netzwerk auf der Basis einer vSphere-Portgruppe. Ein externes Netzwerk stellt für virtuelle Maschinen, die mit externen Organisationen verbunden sind, die Schnittstelle zum Internet bereit.

Weitere Informationen zu Organisationsnetzwerken erhalten Sie unter „Grundlagen zu Organisationsnetzwerken“, auf Seite 33.

Hinzufügen eines externen Netzwerks

Fügen Sie der Umgebung ein externes Netzwerk hinzu, um vSphere-Netzwerkressourcen zur Verwendung in vCloud Director zu registrieren. Sie können Organisationsnetzwerke erstellen, die eine Verbindung zu externen Netzwerken herstellen.

Voraussetzungen

Eine Portgruppe in vSphere ist verfügbar. Wenn die Portgruppe VLAN verwendet, kann sie nur ein einziges VLAN verwenden. Portgruppen mit VLAN-Trunking werden nicht unterstützt.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Externe Netzwerke]** .

2 Klicken Sie auf die Schaltfläche **[Netzwerk hinzufügen]** .

3 Wählen Sie einen vCenter Server und eine vSphere-Portgruppe aus und klicken Sie dann auf **[Weiter]** .

4 Geben Sie die Netzwerkeinstellungen ein und klicken Sie dann auf **[Weiter]** .

5 Geben Sie einen Namen und ggf. eine Beschreibung (optional) für das Netzwerk ein und klicken Sie dann auf **[Weiter]** .

6 Überprüfen Sie die Netzwerkeinstellungen und klicken Sie auf **[Fertigstellen]** .

Weiter

Sie können nun ein Organisationsnetzwerk erstellen, das eine Verbindung zu dem externen Netzwerk herstellt.

Netzwerkpools

Bei einem Netzwerkpool handelt es sich um eine Gruppe undifferenzierter Netzwerke, die in einem Organisations-vDC für die Erstellung von vApp-Netzwerken und bestimmten Typen von Organisationsnetzwerken zur Verfügung gestellt werden.

Netzwerkpools werden durch vSphere-Netzwerkressourcen wie VLAN-IDs, Portgruppen bzw. cloudisolierte Netzwerke gestützt. In vCloud Director werden anhand von Netzwerkpools Organisationsnetzwerke mit NAT-Routing und interne Organisationsnetzwerke sowie alle vApp-Netzwerke erstellt. Der Datenverkehr in den einzelnen Netzwerken wird auf der Ebene von Layer 2 von allen anderen Netzwerken isoliert.

Jedes Organisations-vDC in vCloud Director kann über einen Netzwerkpool verfügen. Mehrere Organisations-vDCs können denselben Netzwerkpool nutzen. Der Netzwerkpool für ein Organisations-vDC stellt die Netzwerke bereit, die erstellt wurden, um das Netzwerkkontingent für ein Organisations-vDC zu erfüllen.

Hinzufügen eines Netzwerkpools, der durch VLAN-IDs gestützt wird

Sie können einen VLAN-gestützten Netzwerkpool hinzufügen, um vSphere-VLAN-IDs zur Verwendung in vCloud Director zu registrieren. VLAN-basierte Netzwerkpools bieten beste Sicherheit, Skalierbarkeit und Systemleistung für Organisationsnetzwerke.

Voraussetzungen

Prüfen Sie, ob eine Reihe von VLAN-IDs und ein vSphere Distributed Switch in vSphere vorhanden sind. Bei den VLAN-IDs muss es sich um gültige IDs handeln, die in dem Switch-Gerät, an das die ESX/ESXi-Server angeschlossen sind, konfiguriert sind.

VORSICHT Die VLANs müssen auf der Ebene von Layer 2 isoliert sein. Wenn die VLANs nicht ordnungsgemäß isoliert sind, kann die Netzwerkkonnektivität beeinträchtigt bzw. unterbrochen werden.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Netzwerkpools]** .
2. Klicken Sie auf **[Netzwerkpool hinzufügen]** .
3. Wählen Sie die Option **[VLAN-basiert]** und klicken Sie dann auf **[Weiter]** .
4. Geben Sie einen VLAN-ID-Bereich ein und klicken Sie dann auf **[Hinzufügen]** .

   Sie können für jede VLAN-ID ein Netzwerk erstellen.
5. Wählen Sie einen vCenter Server und einen vSphere Distributed Switch aus und klicken Sie dann auf **[Weiter]** .
6. Geben Sie einen Namen und ggf. eine Beschreibung (optional) für das Netzwerk ein und klicken Sie dann auf **[Weiter]** .
7. Überprüfen Sie die Einstellungen für den Netzwerkpool und klicken Sie auf **[Fertigstellen]** .

Weiter

Sie können nun ein Organisationsnetzwerk erstellen, das durch den Netzwerkpool gestützt wird oder Sie können den Netzwerkpool einem Organisations-vDC zuordnen und vApp-Netzwerke erstellen.

Hinzufügen eines Netzwerkpools, der durch cloudisolierte Netzwerke gestützt wird

Sie können einen Netzwerkpool erstellen, der durch cloudisolierte Netzwerke gestützt wird. Ein cloudisoliertes Netzwerk arbeitet hostübergreifend, bietet Datenverkehrisolierung von anderen Netzwerken und eignet sich daher in besonderem Maße für vApp-Netzwerke.

Bei isolationsbasierten Netzwerkpools werden in vSphere keine bereits bestehenden Portgruppen vorausgesetzt.

Voraussetzungen

Prüfen Sie, ob ein vSphere Distributed Switch vorhanden ist.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Netzwerkpools]** .
2. Klicken Sie auf **[Netzwerkpool hinzufügen]** .
3. Wählen Sie die Option **[VCD-Netzwerk isolationsbasiert]** und klicken Sie dann auf **[Weiter]** .
4. Geben Sie die Anzahl an Netzwerken an, die aus dem Netzwerkpool erstellt werden sollen.
5. (Optional) Geben Sie eine VLAN-ID ein.
6. Wählen Sie einen vCenter Server und einen vSphere Distributed Switch aus und klicken Sie dann auf **[Weiter]** .
7. Geben Sie einen Namen und eine Beschreibung (optional) für das Netzwerk ein und klicken Sie dann auf **[Weiter]** .
8. Überprüfen Sie die Einstellungen für den Netzwerkpool und klicken Sie auf **[Fertigstellen]** .

vCloud Director erstellt in vSphere die benötigten cloudisolierten Netzwerke.

Weiter

Sie können nun ein Organisationsnetzwerk erstellen, das durch den Netzwerkpool gestützt wird oder Sie können den Netzwerkpool einem Organisations-vDC zuordnen und vApp-Netzwerke erstellen. Sie können nun auch bei Bedarf den MTU-Wert für den Netzwerkpool erhöhen. Weitere Informationen erhalten Sie unter „Festlegen des MTU-Werts für einen Netzwerkpool, der durch cloudisolierte Netzwerke gestützt wird“, auf Seite 22.

Hinzufügen eines Netzwerkpools, der durch vSphere-Portgruppen gestützt wird

Sie können einen Netzwerkpool hinzufügen, der durch Portgruppen gestützt wird, um vSphere-Portgruppen zur Verwendung in vCloud Director zu registrieren. Im Gegensatz zu den anderen Typen wird bei Netzwerkpools, die durch vSphere-Portgruppen gestützt werden, kein vSphere Distributed Switch benötigt.

Vorsicht Die Portgruppen müssen von allen anderen Portgruppen auf der Ebene von Layer 2 isoliert sein. Die Portgruppen müssen physisch oder unter Verwendung von VLAN-Tags isoliert sein. Wenn die Portgruppen nicht ordnungsgemäß isoliert sind, kann die Netzwerkkonnektivität beeinträchtigt bzw. unterbrochen werden.

Voraussetzungen

Prüfen Sie, ob in vSphere eine oder mehrere Portgruppen verfügbar sind. Die Portgruppen müssen auf allen ESX/ESXi-Hosts in dem Cluster verfügbar sein, und jede Portgruppe darf nur ein einziges VLAN verwenden. Portgruppen mit VLAN-Trunking werden nicht unterstützt.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Netzwerkpools]** .

2 Klicken Sie auf **[Netzwerkpool hinzufügen]** .

3 Wählen Sie die Option **[vSphere portgruppenbasiert]** und klicken Sie dann auf **[Weiter]** .

4 Wählen Sie einen vCenter Server aus und klicken Sie dann auf **[Weiter]** .

5 Wählen Sie eine oder mehrere Portgruppen aus, klicken Sie auf **[Hinzufügen]** und klicken Sie auf **[Weiter]** .

   Sie können für jede Portgruppe ein Netzwerk erstellen.

6 Geben Sie einen Namen und ggf. eine Beschreibung (optional) für das Netzwerk ein und klicken Sie dann auf **[Weiter]** .

7 Überprüfen Sie die Einstellungen für den Netzwerkpool und klicken Sie auf **[Fertigstellen]** .

Weiter

Sie können nun ein Organisationsnetzwerk erstellen, das durch den Netzwerkpool gestützt wird oder Sie können den Netzwerkpool einem Organisations-vDC zuordnen und vApp-Netzwerke erstellen.

Festlegen des MTU-Werts für einen Netzwerkpool, der durch cloudisolierte Netzwerke gestützt wird

Sie können über den MTU-Wert die maximalen Übertragungseinheiten festlegen, die vCloud Director für einen durch cloudisolierte Netzwerke gestützten Netzwerkpool verwendet. MTU ist die größte Datenmenge, die als ein Paket übertragen werden kann, bevor sie in kleinere Pakete aufgeteilt wird.

Wenn Sie das Gastbetriebssystem der virtuellen Maschine und die zugrunde liegende physische Infrastruktur mit dem Standard-MTU-Wert (1500 Byte) konfigurieren, werden Frames vom VMware-Netzwerkisolationsprotokoll fragmentiert. Um diese Fragmentierung zu verhindern, sollten Sie den MTU-Wert für den Netzwerkpool und das zugrunde liegende physische Netzwerk auf mindestens 1524 Byte erhöhen. Sie können für den Netzwerkpool keinen größeren MTU-Wert angeben als für das physische Netzwerk.

Wenn das physische Netzwerk einen MTU-Wert von weniger als 1500 Byte aufweist, verringern Sie den MTU-Wert des Netzwerkpools entsprechend dem Wert des zugrunde liegenden physischen Netzwerks.

Voraussetzungen

Prüfen Sie, ob ein durch cloudisolierte Netzwerke gestützter Netzwerkpool vorhanden ist. Bevor Sie den MTU-Wert für einen Netzwerkpool erhöhen, müssen Sie sicherstellen, dass die physische Switch-Infrastruktur Datenpakete mit einem größeren MTU-Wert als 1500 Byte, so genannte Jumbo-Frames, unterstützt.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Netzwerkpools]** .

2 Klicken Sie mit der rechten Maustaste auf den Netzwerkpoolnamen und wählen Sie den Befehl **[Eigenschaften]** .

3 Geben Sie auf der Registerkarte **[MTU für Netzwerkpool]** den MTU-Wert ein und klicken Sie auf **[OK]** .

vCloud Director ändert den MTU-Wert für den Netzwerkpool und für alle anderen Netzwerkpools, die denselben vSphere Distributed Switch verwenden.

Erstellen und Bereitstellen von Organisationen 3

Organisationen stellen Ressourcen für Gruppen von Benutzern bereit und legen Richtlinien fest, nach denen Benutzer zur Verwendung dieser Ressourcen berechtigt sind. Erstellen Sie eine Organisation für jede Gruppe von Benutzern, für die eigene Ressourcen oder Richtlinien benötigt werden.

Dieses Kapitel behandelt die folgenden Themen:

- „Grundlagen zu Leases“, auf Seite 23
- „Erstellen einer Organisation“, auf Seite 24
- „Zuweisen von Ressourcen zu einer Organisation“, auf Seite 28
- „Hinzufügen von Netzwerken zu einer Organisation“, auf Seite 33

Grundlagen zu Leases

Beim Erstellen von Organisationen müssen u. a. Leases angegeben werden. Leases ermöglichen eine grundlegende Steuerung der Speicher- und Rechenressourcen, indem festgelegt wird, wie lange vApps maximal ausgeführt werden können und ob vApp-Vorlagen gespeichert werden dürfen.

Der Zweck von Laufzeit-Leases besteht darin, zu verhindern, dass inaktive vApps Rechenressourcen verbrauchen. Wenn beispielsweise ein Benutzer eine vApp startet und anschließend verreist, ohne sie anzuhalten, verbraucht die vApp fortlaufend Ressourcen.

Eine Laufzeit-Lease beginnt zu dem Zeitpunkt, an dem der Benutzer eine vApp startet. Wenn die Laufzeit-Lease abläuft, hält vCloud Director die vApp an.

Der Zweck von Speicher-Leases besteht darin, zu verhindern, dass nicht verwendete vApps und vApp-Vorlagen Speicherressourcen verbrauchen. Eine vApp-Speicher-Lease beginnt zu dem Zeitpunkt, an dem der Benutzer eine vApp anhält. Speicher-Leases haben keine Auswirkungen auf ausgeführte vApps. Eine vApp-Vorlagen-Speicher-Lease beginnt, wenn der Benutzer die vApp-Vorlage einer vApp oder einem Arbeitsbereich hinzufügt oder sie herunterlädt, kopiert oder verschiebt.

Bei Ablauf der Speicher-Lease kennzeichnet vCloud Director die vApp bzw. vApp-Vorlage als abgelaufen oder löscht sie entsprechend den festgelegten Organisationsrichtlinien.

Weitere Informationen zum Festlegen der Leases erhalten Sie unter „Konfigurieren der Einstellungen von Organisations-Leases, -Kontingenten und -Grenzwerten“, auf Seite 27.

Die Benutzer können ihre Voreinstellungen so konfigurieren, dass ihnen vor Ablauf der Laufzeit- oder Speicher-Lease eine Benachrichtigungs-E-Mail zugesendet wird. Weitere Informationen zu den Benutzereinstellungen zum Ablauf der Leases erhalten Sie unter „Festlegen der Benutzereinstellungen“, auf Seite 14.

Erstellen einer Organisation

Beim Erstellen einer Organisation werden die Organisationseinstellungen festgelegt und ein Benutzerkonto für den Organisationsadministrator angelegt.

Vorgehensweise

1 Öffnen des Assistenten für neue Organisationen auf Seite 24

Öffnen Sie den Assistenten für neue Organisationen, um den Vorgang zum Erstellen einer Organisation zu starten.

2 Festlegen eines Namens für die Organisation auf Seite 25

Geben Sie einen beschreibenden Namen und bei Bedarf eine Beschreibung für Ihre neue Organisation ein.

3 Festlegen der LDAP-Optionen für die Organisation auf Seite 25

Sie können einen LDAP-Dienst als Verzeichnis für Benutzer und Gruppen in der Organisation nutzen. Wenn Sie keinen LDAP-Dienst angeben, müssen Sie die Benutzerkonten für die Benutzer in der Organisation einzeln erstellen. Die LDAP-Optionen können ausschließlich von einem Systemadministrator festgelegt werden. Organisationsadministratoren verfügen nicht über die erforderlichen Berechtigungen, diese Optionen zu bearbeiten.

4 Hinzufügen von lokalen Benutzern zur Organisation auf Seite 26

Alle Organisationen sollten über mindestens ein lokales, nicht an LDAP gebundenes Organisationsadministratorkonto verfügen, mit dem sich die Benutzer auch dann anmelden können, wenn der LDAP-Dienst nicht verfügbar ist.

5 Festlegen der Richtlinie zur Veröffentlichung von Katalogen für eine Organisation auf Seite 26

Über einen Katalog wird den Benutzern von Organisationen eine Bibliothek von vApp-Vorlagen und Medien bereitgestellt, die die Benutzer zum Erstellen von vApps und zur Installation von Anwendungen auf virtuellen Maschinen nutzen können.

6 Konfigurieren der E-Mail-Einstellungen auf Seite 27

vCloud Director benötigt einen SMTP-Server, um E-Mails zur Benachrichtigung von Benutzern und zu Systemwarnungen zu versenden. Organisationen können die systemweit geltenden E-Mail-Einstellungen oder eigene systemunabhängige Einstellungen verwenden.

7 Konfigurieren der Einstellungen von Organisations-Leases, -Kontingenten und -Grenzwerten auf Seite 27

Leases, Kontingente und Grenzwerte beschränken die Möglichkeit von Benutzern in der Organisation zur Nutzung von Speicher- und Prozessorressourcen. Verwenden Sie diese Einstellungen, um zu verhindern, dass einzelne Benutzer eine Ressource der Organisation erschöpfend oder ausschließlich nutzen.

8 Bestätigen der Einstellungen und Erstellen der Organisation auf Seite 28

Überprüfen Sie die eingegebenen Einstellungen, bevor Sie die Organisation erstellen.

Öffnen des Assistenten für neue Organisationen

Öffnen Sie den Assistenten für neue Organisationen, um den Vorgang zum Erstellen einer Organisation zu starten.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationen]** .

2 Klicken Sie auf die Schaltfläche **[Neue Organisation]** .

Der Assistent für neue Organisationen wird gestartet.

Festlegen eines Namens für die Organisation

Geben Sie einen beschreibenden Namen und bei Bedarf eine Beschreibung für Ihre neue Organisation ein.

Vorgehensweise

1 Geben Sie einen Organisationsnamen ein.

Dieser Name ist eine eindeutige Kennung, die Teil der URL ist, über die sich die Benutzer der Organisation bei der Organisation anmelden.

2 Geben Sie einen Anzeigenamen für die Organisation ein.

Dieser Name wird in der Kopfzeile des Browsers angezeigt, wenn sich Benutzer der Organisation über die eindeutige URL bei vCloud Director anmelden. Dieser Name kann später von einem Administrator oder Organisationsadministrator geändert werden.

3 (Optional) Geben Sie eine Beschreibung der Organisation ein.

4 Klicken Sie auf **[Weiter]** .

Festlegen der LDAP-Optionen für die Organisation

Sie können einen LDAP-Dienst als Verzeichnis für Benutzer und Gruppen in der Organisation nutzen. Wenn Sie keinen LDAP-Dienst angeben, müssen Sie die Benutzerkonten für die Benutzer in der Organisation einzeln erstellen. Die LDAP-Optionen können ausschließlich von einem Systemadministrator festgelegt werden. Organisationsadministratoren verfügen nicht über die erforderlichen Berechtigungen, diese Optionen zu bearbeiten.

Weitere Informationen zur Eingabe der LDAP-Einstellungen erhalten Sie unter „Konfigurieren der System-LDAP-Einstellungen“, auf Seite 108.

Vorgehensweise

1 Wählen Sie die Quelle für Benutzer der Organisation aus.

Option	Beschreibung
LDAP nicht verwenden	Der Administrator der Organisation erstellt für alle Benutzer der Organisation ein lokales Benutzerkonto. Wenn Sie diese Option wählen, können Sie keine Gruppen erstellen.
LDAP-Dienst des VCD-Systems	Verwendet den LDAP-Dienst des vCloud Director-Systems als Quelle für Benutzer und Gruppen der Organisation.
LDAP-Dienst anpassen	Verbindet die Organisation mit ihrem eigenen, privaten LDAP-Dienst.

2 Geben Sie weitere Daten an, die für die ausgewählte Option erforderlich sind.

Option	Aktion
LDAP nicht verwenden	Klicken Sie auf **[Weiter]** .
LDAP-Dienst des VCD-Systems	(Optional) Geben Sie den distinktiven Namen (DN) der zu verwendenden Organisationseinheit (OU) ein, um die Menge der in die Organisation zu importierenden Benutzer einzuschränken, und klicken Sie dann auf **[Weiter]** . Wenn Sie keinen Wert eingeben, können alle Benutzer in dem System-LDAP-Dienst in die Organisation importiert werden. **Hinweis** Die Festlegung einer Organisationseinheit schränkt nicht die importierbaren LDAP-Gruppen ein. Sie können beliebige LDAP-Gruppen aus dem Root-Verzeichnis des System-LDAP-Verzeichnisses importieren. Allerdings können sich nur Benutzer, die sich in der Organisationseinheit und in der importierten Gruppe befinden, bei der Organisation anmelden.
LDAP-Dienst anpassen	Klicken Sie auf **[Weiter]** und geben Sie die benutzerdefinierten LDAP-Einstellungen für die Organisation ein.

Hinzufügen von lokalen Benutzern zur Organisation

Alle Organisationen sollten über mindestens ein lokales, nicht an LDAP gebundenes Organisationsadministratorkonto verfügen, mit dem sich die Benutzer auch dann anmelden können, wenn der LDAP-Dienst nicht verfügbar ist.

Vorgehensweise

1 Klicken Sie auf **[Hinzufügen]** .

2 Geben Sie einen Benutzernamen und ein Kennwort ein.

3 Weisen Sie dem Benutzer die gewünschte Rolle zu.

4 (Optional) Geben Sie die Kontaktdaten für den neuen Benutzer ein.

5 Wählen Sie **[Unbegrenzt]** aus, oder geben Sie ein Benutzerkontingent für gespeicherte und laufende virtuelle Maschinen ein, und klicken Sie auf **[OK]** .

   Mit einer solchen Kontingentfestlegung wird für den Benutzer die Möglichkeit zur Beanspruchung von Speicherplatz und Rechenressourcen in der Organisation eingeschränkt.

6 Klicken Sie auf **[Weiter]** .

Festlegen der Richtlinie zur Veröffentlichung von Katalogen für eine Organisation

Über einen Katalog wird den Benutzern von Organisationen eine Bibliothek von vApp-Vorlagen und Medien bereitgestellt, die die Benutzer zum Erstellen von vApps und zur Installation von Anwendungen auf virtuellen Maschinen nutzen können.

Im Allgemeinen stehen Kataloge nur den Benutzern in einer einzigen Organisation zur Verfügung; Systemadministratoren können jedoch Organisationsadministratoren erlauben, eigene Kataloge für alle Organisationen in der vCloud Director-Installation zu veröffentlichen.

Vorgehensweise

1 Wählen Sie eine Option zur Katalogveröffentlichung aus.

Option	Beschreibung
Kataloge können nicht veröffentlicht werden	Der Organisationsadministrator kann für Benutzer außerhalb seiner Organisation keine Kataloge veröffentlichen.
Veröffentlichung von Katalogen bei allen Organisationen zulassen	Der Organisationsadministrator kann Kataloge für Benutzer in allen Organisationen veröffentlichen.

2 Klicken Sie auf **[Weiter]** .

Konfigurieren der E-Mail-Einstellungen

vCloud Director benötigt einen SMTP-Server, um E-Mails zur Benachrichtigung von Benutzern und zu Systemwarnungen zu versenden. Organisationen können die systemweit geltenden E-Mail-Einstellungen oder eigene systemunabhängige Einstellungen verwenden.

Vorgehensweise

1 Wählen Sie eine Option zu dem SMTP-Server aus.

Option	Beschreibung
Standard-SMTP-Server des Systems verwenden	Die Organisation verwendet den Standard-SMTP-Server des Systems.
SMTP-Server der Organisation festlegen	Die Organisation verwendet einen eigenen SMTP-Server. Geben Sie den DNS-Hostnamen oder die IP-Adresse des SMTP-Servers sowie die Portnummer ein. (Optional) Aktivieren Sie das Kontrollkästchen **[Authentifizierung erforderlich]** und geben Sie einen Benutzernamen und das zugehörige Kennwort ein.

2 Wählen Sie eine Option zu den Benachrichtigungseinstellungen aus.

Option	Beschreibung
Standard-Benachrichtigungseinstellungen des Systems verwenden	Die Organisation verwendet die Benachrichtigungseinstellungen des Systems.
Benachrichtigungseinstellungen der Organisation festlegen	Die Organisation verwendet eigene Benachrichtigungseinstellungen. Geben Sie eine E-Mail-Adresse ein, die als Absender für E-Mails der Organisation angezeigt wird, geben Sie desgleichen einen Text als Betreff ein und wählen Sie die Empfänger aus.

3 (Optional) Geben Sie eine Ziel-E-Mail-Adresse ein und klicken Sie auf **[E-Mail-Einstellungen testen]** , um zu überprüfen, ob die konfigurierten SMTP-Servereinstellungen wie erwartet funktionieren.

4 Klicken Sie auf **[Weiter]** .

Konfigurieren der Einstellungen von Organisations-Leases, -Kontingenten und -Grenzwerten

Leases, Kontingente und Grenzwerte beschränken die Möglichkeit von Benutzern in der Organisation zur Nutzung von Speicher- und Prozessorressourcen. Verwenden Sie diese Einstellungen, um zu verhindern, dass einzelne Benutzer eine Ressource der Organisation erschöpfend oder ausschließlich nutzen.

Weitere Informationen zu Leases erhalten Sie unter „Grundlagen zu Leases“, auf Seite 23.

Vorgehensweise

1 Wählen Sie die gewünschten Lease-Optionen für vApps und vApp-Vorlagen aus.

Leases ermöglichen eine grundlegende Steuerung der Speicher- und Rechenressourcen einer Organisation, indem festgelegt wird, wie lange vApps maximal ausgeführt und wie lange vApps und vApp-Vorlagen gespeichert werden können. Darüber hinaus können Sie festlegen, was mit den vApps bzw. vApp-Vorlagen geschieht, wenn der Speicher-Lease abläuft.

2 Wählen Sie die Kontingente für laufende und gespeicherte virtuelle Maschinen aus.

Kontingente legen fest, wie viele virtuelle Maschinen die einzelnen Benutzer in der Organisation in deren virtuellen Datencentern speichern und einschalten dürfen. Die festgelegten Kontingente werden für alle der Organisation neu hinzugefügten Benutzer als Standardwerte übernommen.

3 Wählen Sie die Grenzwerte für ressourcenintensive Operationen aus.

Bestimmte vCloud Director-Operationen, beispielsweise das Kopieren und Verschieben, verbrauchen mehr Ressourcen als andere. Mit diesen Grenzwerten können Sie verhindern, dass ressourcenintensive Operationen Auswirkungen auf alle anderen Benutzer in einer Organisation haben. Darüber hinaus bieten diese Grenzwerte einen Schutz gegen DoS-Angriffe.

4 Wählen Sie die Anzahl gleichzeitiger VMware Remote-Konsole-Verbindungen für alle virtuellen Maschinen aus.

Möglicherweise möchten Sie die Anzahl gleichzeitiger Verbindungen aus Gründen der Systemleistung oder aus Sicherheitsgründen beschränken.

HINWEIS Diese Einstellung gilt nicht für VNC- (Virtual Network Computing-) und RDP- (Remote Desktop Protocol-)Verbindungen.

5 (Optional) Aktivieren Sie das Kontrollkästchen **[Kontosperrung aktiviert]** und wählen Sie die Anzahl der akzeptierten ungültigen Anmeldeversuche vor Sperrung eines Benutzerkontos sowie das Sperrungsintervall aus.

6 Klicken Sie auf **[Weiter]** .

Bestätigen der Einstellungen und Erstellen der Organisation

Überprüfen Sie die eingegebenen Einstellungen, bevor Sie die Organisation erstellen.

Vorgehensweise

1 Überprüfen Sie die Einstellungen für die Organisation.

2 (Optional) Klicken Sie auf **[Zurück]** , wenn Sie die Einstellungen ändern möchten.

3 Klicken Sie auf **[Fertigstellen]** , um die Einstellungen zu übernehmen und die Organisation zu erstellen.

Weiter

Weisen Sie der Organisation Ressourcen zu.

Zuweisen von Ressourcen zu einer Organisation

Sie können Organisationen Ressourcen zuweisen, indem Sie ein Organisations-vDC erstellen, das von einem Provider-vDC abgetrennt ist. Jede Organisation kann über mehrere Organisations-vDCs verfügen.

Voraussetzungen

Sie können Organisationen erst dann Ressourcen zuweisen, wenn ein Provider-vDC eingerichtet ist.

Vorgehensweise

1 Öffnen des Assistenten für die Zuweisung von Ressourcen auf Seite 29

Öffnen Sie den Assistenten für die Zuweisung von Ressourcen, um den Vorgang zum Erstellen eines Organisations-vDC für eine Organisation zu starten.

2 Auswählen eines Provider-vDC auf Seite 29

Organisations-vDCs erhalten ihre Rechen- und Arbeitsspeicherressourcen von einem Provider-vDC. Das Organisations-vDC stellt diese Ressourcen vApps und virtuellen Maschinen in der Organisation zur Verfügung.

3 Auswählen eines Zuweisungsmodells auf Seite 30

Über das Zuweisungsmodell wird festgelegt, auf welche Weise und zu welchem Zeitpunkt das Provider-vDC die von Ihnen zugewiesenen Rechen- und Arbeitsspeicherressourcen den Organisations-vDCs zusichert.

4 Konfigurieren des Zuweisungsmodells auf Seite 30

Sie konfigurieren das Zuweisungsmodell, indem Sie eine Menge von Provider-vDC-Ressourcen angeben, die dem Organisations-vDC zugewiesen werden soll.

5 Zuweisen von Speicher auf Seite 31

Organisations-vDCs benötigen Speicherplatz für vApps und vApp-Vorlagen. Sie können Speicher zuweisen, der über die Provider-vDC-Datenspeicher zur Verfügung steht.

6 Auswählen eines Netzwerkpools auf Seite 32

Bei einem Netzwerkpool handelt es sich um eine Gruppe undifferenzierter Netzwerke, die zur Erstellung von vApp-Netzwerken und NAT-geleiteten oder internen Organisationsnetzwerken verwendet werden.

7 Festlegen eines Namens für das Organisations-vDC auf Seite 32

Sie können einen beschreibenden Namen und eine optionale Beschreibung bereitstellen, um die für das neue Organisations-vDC verfügbaren vSphere-Funktionen anzugeben.

8 Bestätigen der Einstellungen und Erstellen des Organisations-vDCs auf Seite 32

Überprüfen Sie die eingegebenen Einstellungen, bevor Sie das neue Organisations-vDC erstellen.

Weiter

Fügen Sie der Organisation ein Netzwerk hinzu.

Öffnen des Assistenten für die Zuweisung von Ressourcen

Öffnen Sie den Assistenten für die Zuweisung von Ressourcen, um den Vorgang zum Erstellen eines Organisations-vDC für eine Organisation zu starten.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationen]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen der Organisation und wählen Sie den Befehl **[Ressourcen zuweisen]** .

Der Assistent für die Zuweisung von Ressourcen wird gestartet.

Auswählen eines Provider-vDC

Organisations-vDCs erhalten ihre Rechen- und Arbeitsspeicherressourcen von einem Provider-vDC. Das Organisations-vDC stellt diese Ressourcen vApps und virtuellen Maschinen in der Organisation zur Verfügung.

Vorgehensweise

1 Wählen Sie ein Provider-vDC aus.

In der Liste der Provider-vDCs werden Informationen zu verfügbaren Ressourcen und in der Netzwerkliste für das ausgewählte Provider-vDC Informationen zu verfügbaren Netzwerken angezeigt.

2 Klicken Sie auf **[Weiter]** .

Auswählen eines Zuweisungsmodells

Über das Zuweisungsmodell wird festgelegt, auf welche Weise und zu welchem Zeitpunkt das Provider-vDC die von Ihnen zugewiesenen Rechen- und Arbeitsspeicherressourcen den Organisations-vDCs zusichert.

Vorgehensweise

1 Wählen Sie ein Zuweisungsmodell aus.

Option	Beschreibung
Zuweisungspool	Nur ein Teil der von Ihnen zugewiesenen Ressourcen wird dem Organisations-vDC zugesichert. Sie können Ressourcen überbelegen, indem Sie den Prozentsatz angeben.
Pay-As-You-Go	Ressourcen werden erst zugesichert, wenn Benutzer in dem Organisations-vDC vApps erstellen. Sie können Ressourcen überbelegen, indem Sie den Prozentsatz der garantierten Ressourcen angeben. Sie können ein Pay-As-You-Go-Organisations-vDC „elastisch" machen, indem Sie mehrere Ressourcenpools zu seinem Provider-vDC hinzufügen.
Reservierungspool	Alle von Ihnen zugewiesenen Ressourcen werden dem Organisations-vDC sofort zugesichert. Die Benutzer in der Organisation können die Überbelegung steuern, indem sie Reservierungs-, Grenzwert- und Prioritätseinstellungen für einzelne virtuelle Maschinen festlegen.

2 Klicken Sie auf **[Weiter]** .

Konfigurieren des Zuweisungsmodells

Sie konfigurieren das Zuweisungsmodell, indem Sie eine Menge von Provider-vDC-Ressourcen angeben, die dem Organisations-vDC zugewiesen werden soll.

Vorgehensweise

1 Wählen Sie die Optionen für Zuweisungsmodelle aus.

Es sind nicht für jedes Modell alle Optionen verfügbar.

Option	Aktion
CPU-Zuweisung	Geben Sie die maximale Menge an Prozessorleistung in GHz an, die den virtuellen Maschinen in dem Organisations-vDC zugewiesen werden soll.
Garantierte CPU-Ressourcen	Geben Sie den Prozentsatz der Prozessorleistung an, die den virtuellen Maschinen in dem Organisations-vDC garantiert werden soll. Sie können Ressourcen überbelegen, indem Sie weniger als 100 % garantieren.
Arbeitsspeicherzuweisung	Geben Sie die maximale Arbeitsspeichermenge in GB an, die den virtuellen Maschinen in dem Organisations-vDC zugewiesen werden soll.
Garantierte Arbeitsspeicherressourcen	Geben Sie den Prozentsatz des Arbeitsspeichers an, der den virtuellen Maschinen in dem Organisations-vDC garantiert werden soll. Sie können Ressourcen überbelegen, indem Sie weniger als 100 % garantieren.
vCPU-Geschwindigkeit	Geben Sie die vCPU-Geschwindigkeit in GHz ein. Anschließend wird den virtuellen Maschinen in dem Organisations-vDC dieser Wert in GHz pro vCPU zugewiesen.
Maximale Anzahl der VMs	Geben Sie die maximale Anzahl virtueller Maschinen an, die in diesem Organisations-vDC erstellt werden dürfen.

2 Klicken Sie auf **[Weiter]** .

Beispiel: Konfigurieren eines Zuweisungsmodells

Wenn Sie ein Organisations-vDC anlegen, erstellt vCloud Director auf der Basis der festgelegten Einstellungen des Zuweisungsmodells einen vSphere-Ressourcenpool. Siehe Tabelle 3-1, Tabelle 3-2 und Tabelle 3-3.

Tabelle 3-1. Auswirkungen der Einstellungen für den Zuweisungspool auf die Einstellungen für den Ressourcenpool

Zuweisungspooleinstellung	Zuweisungspoolwert	Ressourcenpooleinstellung	Ressourcenpoolwert
CPU-Zuweisung	25 GHz	CPU-Limit	25 GHz
CPU % garantiert	10 %	CPU-Reservierung	2,5 GHz
Arbeitsspeicherzuweisung	50 GB	Arbeitsspeicher-Limit	50 GB
Arbeitsspeicher % garantiert	20 %	Arbeitsspeicherreservierung	10 GB

Tabelle 3-2. Auswirkungen der Pay-As-You-Go-Einstellungen auf die Einstellungen für den Ressourcenpool

Pay-As-You-Go-Einstellung	Pay-As-You-Go-Wert	Ressourcenpooleinstellung	Ressourcenpoolwert
CPU % garantiert	10 %	CPU-Reservierung, CPU-Limit	0,00 GHz, Unbegrenzt
Arbeitsspeicher % garantiert	100 %	Arbeitsspeicherreservierung, Arbeitsspeicher-Limit	0,00 GB, Unbegrenzt

Für Ressourcenpools, die Pay-As-You-Go-Organisations-vDCs unterstützen, können weder Reservierungen noch Grenzwerte angegeben werden. Pay-As-You-Go-Einstellungen betreffen ausschließlich die Überbelegung. Eine Garantie von 100 % bedeutet, dass keine Überbelegung möglich ist. Je niedriger der Prozentsatz, desto mehr Überbelegung ist möglich.

Tabelle 3-3. Auswirkungen der Einstellungen für den Reservierungspool auf die Einstellungen für den Ressourcenpool

Reservierungspooleinstellung	Reservierungspoolwert	Ressourcenpooleinstellung	Ressourcenpoolwert
CPU-Zuweisung	25 GHz	CPU-Reservierung, CPU-Limit	25 GHz, 25 GHz
Arbeitsspeicherzuweisung	50 GB	Arbeitsspeicherreservierung, Arbeitsspeicher-Limit	50 GB, 50 GB

Zuweisen von Speicher

Organisations-vDCs benötigen Speicherplatz für vApps und vApp-Vorlagen. Sie können Speicher zuweisen, der über die Provider-vDC-Datenspeicher zur Verfügung steht.

Durch den Einsatz von Thin Provisioning kann die Zuweisung von übermäßigem Speicher vermieden werden, und generell kann Speicherplatz gespart werden. Für eine virtuelle Maschine mit einer „schlanken“ virtuellen Festplatte stellt ESX/ESXi den gesamten Speicherplatz bereit, der für aktuelle und künftige Operationen der Festplatte benötigt wird. ESX/ESXi übergibt jedoch nur so viel Speicherplatz, wie die Festplatte für den anfänglichen Betrieb benötigt.

Bei Fast Provisioning wird dadurch Zeit eingespart, dass für bestimmte Operationen von vSphere untereinander verbundene Klone verwendet werden. Weitere Informationen erhalten Sie unter „Fast Provisioning virtueller Maschinen“, auf Seite 95.

WICHTIG Fast Provisioning erfordert vCenter Server 5.0 und ESXi 5.0-Hosts. Wenn das Provider-vDC, auf dem das Organisations-vDC basiert, ESX/ESXi 4.x-Hosts enthält, müssen Sie Fast Provisioning deaktivieren. Wenn das Provider-vDC, auf dem das Organisations-vDC basiert, mit mehr als acht Hosts verbundene VMFS-Datenspeicher enthält, kann das Einschalten von virtuellen Maschinen fehlschlagen. Stellen Sie sicher, dass die Datenspeicher mit maximal acht Hosts verbunden sind.

Vorgehensweise

1 Geben Sie das zuzuweisende Speichervolumen ein.

2 (Optional) Mit dem Kontrollkästchen **[Thin Provisioning aktivieren]** können Sie die „schlanke Speicherzuweisung“ für virtuelle Maschinen in dem Organisations-vDC aktivieren.

3 (Optional) Mit dem Kontrollkästchen **[Fast Provisioning aktivieren]** können Sie die „schnelle Bereitstellung“ für virtuelle Maschinen in dem Organisations-vDC deaktivieren.

4 Klicken Sie auf **[Weiter]** .

Auswählen eines Netzwerkpools

Bei einem Netzwerkpool handelt es sich um eine Gruppe undifferenzierter Netzwerke, die zur Erstellung von vApp-Netzwerken und NAT-geleiteten oder internen Organisationsnetzwerken verwendet werden.

Vorgehensweise

1 Wählen Sie einen Netzwerkpool aus oder wählen Sie die Option **[Keine]** .

Wenn Sie die Option **[Keine]** wählen, können Sie zu einem späteren Zeitpunkt einen Netzwerkpool hinzufügen.

2 Geben Sie die maximale Anzahl an Netzwerken ein, die die Organisation aus dem Netzwerkpool bereitstellen kann.

3 Klicken Sie auf **[Weiter]** .

Festlegen eines Namens für das Organisations-vDC

Sie können einen beschreibenden Namen und eine optionale Beschreibung bereitstellen, um die für das neue Organisations-vDC verfügbaren vSphere-Funktionen anzugeben.

Vorgehensweise

1 Geben Sie einen Namen und bei Bedarf eine Beschreibung ein.

2 Klicken Sie auf **[Weiter]** .

Bestätigen der Einstellungen und Erstellen des Organisations-vDCs

Überprüfen Sie die eingegebenen Einstellungen, bevor Sie das neue Organisations-vDC erstellen.

Vorgehensweise

1 Überprüfen Sie die Einstellungen für das Organisations-vDC.

2 (Optional) Klicken Sie auf **[Zurück]** , wenn Sie die Einstellungen ändern möchten.

3 Klicken Sie auf **[Fertigstellen]** , um die Einstellungen zu übernehmen und das Organisations-vDC zu erstellen.

Wenn Sie ein Organisations-vDC anlegen, erstellt vCloud Director in vSphere einen Ressourcenpool, über den Prozessor- und Arbeitsspeicherressourcen bereitgestellt werden.

Hinzufügen von Netzwerken zu einer Organisation

Fügen Sie Ihrer Organisation ein Netzwerk hinzu, über das die virtuellen Maschinen miteinander Daten austauschen können und über das ein Internetzugang bereitgestellt werden kann. Jede Organisation kann über mehrere Organisationsnetzwerke verfügen.

Grundlagen zu Organisationsnetzwerken

Organisationsnetzwerke ermöglichen es virtuellen Maschinen, Daten innerhalb einer Organisation miteinander auszutauschen und auf das Internet zuzugreifen. Organisationsnetzwerke benötigen ein externes Netzwerk, einen Netzwerkpool oder beides.

Tabelle 3-4 enthält eine Beschreibung der Arten von Organisationsnetzwerken.

Tabelle 3-4. Arten von Organisationsnetzwerken und ihre Voraussetzungen

Organisationsnetzwerktyp	Beschreibung	Voraussetzungen
Externes Organisationsnetzwerk – direkte Verbindung	Ermöglicht den Zugriff durch mehrere Organisationen. Zu verschiedenen Organisationen gehörende VMs können sich mit diesem Netzwerk verbinden und den Datenverkehr dieses Netzwerkes sehen. Dieses Netzwerk stellt die direkte Layer-2-Konnektivität für Rechner außerhalb der Organisation zur Verfügung. Computer außerhalb dieser Organisation können direkt eine Verbindung zu den Computern in der Organisation herstellen.	Externes Netzwerk
Externes Organisationsnetzwerk – Verbindung mit NAT-Routing	Ermöglicht den Zugriff nur durch diese Organisation. Nur virtuelle Maschinen in dieser Organisation können sich mit diesem Netzwerk verbinden. Dieses Netzwerk bietet auch den kontrollierten Zugriff auf ein externes Netzwerk. Die System- und Organisationsadministratoren können das NAT-Modul und die Firewall-Einstellungen so konfigurieren, dass der Zugriff vom externen Netzwerk auf ausgewählte virtuelle Maschinen ermöglicht wird.	Externes Netzwerk und Netzwerkpool
Internes Organisationsnetzwerk	Ermöglicht den Zugriff nur durch diese Organisation. Nur virtuelle Maschinen in dieser Organisation können sich mit diesem Netzwerk verbinden und den Datenverkehr in diesem Netzwerk sehen. Dieses Netzwerk stellt ein isoliertes, privates Netzwerk für eine Organisation bereit, mit dem sich mehrere vApps verbinden können. Dieses Netzwerk bietet keine Konnektivität für Rechner außerhalb dieser Organisation. Computer außerhalb dieser Organisation können keine Verbindung zu den Computern in der Organisation herstellen.	Netzwerkpool

Hinzufügen eines externen, direkten Organisationsnetzwerks

Sie können ein externes, direktes Organisationsnetzwerk hinzufügen, auf das mehrere Organisationen zugreifen können. Sie stellen normalerweise über das externe Netzwerk eine Verbindung zum Internet her. Die Organisation stellt die Verbindung zu diesem Netzwerk direkt her.

Voraussetzungen

Prüfen Sie, ob ein externes Netzwerk vorhanden ist.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationen]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen der Organisation und wählen Sie den Befehl **[Netzwerke hinzufügen]** .

3 Wählen Sie den gewünschten Einrichtungstyp und den Netzwerktyp aus und klicken Sie dann auf **[Weiter]** .

Sie können beide Verfahren verwenden, um ein externes, direktes Organisationsnetzwerk zu erstellen.

Option	Netzwerktyp
Typisch	Aktivieren Sie das Kontrollkästchen für das externe Netzwerk und wählen Sie aus dem Dropdown-Menü die Option **[Direkte Verbindung]** .
Erweitert	Wählen Sie die Option **[Externes Organisationsnetzwerk – direkte Verbindung]** .

4 Wählen Sie ein externes Netzwerk aus und klicken Sie dann auf **[Weiter]** .

Wenn Sie das Kontrollkästchen **[Nur Netzwerke verwenden, auf die diese Organisation zugreifen kann]** deaktivieren, werden auch externe Netzwerke angezeigt, die der Organisation aktuell nicht durch ihre Organisations-vDCs verfügbar gemacht wurden. Wenn Sie dieses Kontrollkästchen deaktivieren, können Sie ein beliebiges Netzwerk auswählen und später ein Organisations-vDC erstellen, das auf das Netzwerk zugreifen kann.

5 Geben Sie einen Namen und bei Bedarf eine Beschreibung ein und klicken Sie dann auf **[Weiter]** .

6 Überprüfen Sie die Einstellungen für das Organisationsnetzwerk.

Klicken Sie auf **[Fertigstellen]** , um die Einstellungen zu übernehmen und das Organisationsnetzwerk zu erstellen, oder klicken Sie auf **[Zurück]** , um die Einstellungen zu bearbeiten.

Hinzufügen eines externen Organisationsnetzwerks mit NAT-Routing

Sie können der Umgebung ein externes Organisationsnetzwerk mit NAT-Routing hinzufügen, für das der Zugriff auf diese Organisation beschränkt ist. Ein externes Organisationsnetzwerk mit NAT-Routing bietet Geräten außerhalb der Organisation NAT-Konnektivität, wodurch die Kontrollmöglichkeiten der Zugriffsberechtigungen verbessert werden.

Voraussetzungen

Prüfen Sie, ob ein externes Netzwerk und ein Netzwerkpool vorhanden sind.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationen]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen der Organisation und wählen Sie den Befehl **[Netzwerke hinzufügen]** .

3 Wählen Sie den gewünschten Einrichtungstyp und den Netzwerktyp aus und klicken Sie dann auf **[Weiter]** .

Sie können beide Verfahren verwenden, um ein externes Organisationsnetzwerk mit Routing zu erstellen.

Option	Netzwerktyp
Typisch	Aktivieren Sie das Kontrollkästchen „Externes Netzwerk“ und wählen Sie aus dem Dropdown-Menü die Option **[Weitergeleitete Verbindung]** .
Erweitert	Wählen Sie die Option **[Externes Organisationsnetzwerk – Verbindung mit NAT-Routing]** .

4 Wählen Sie ein externes Netzwerk und einen Netzwerkpool aus und klicken Sie dann auf **[Weiter]** .

5 (Optional) Deaktivieren Sie das Kontrollkästchen **[Nur Netzwerke verwenden, auf die diese Organisation zugreifen kann]** , um externe Netzwerke und Netzwerkpools anzuzeigen, die der Organisation derzeit nicht über ihre Organisations-vDCs zur Verfügung stehen.

Wenn Sie dieses Kontrollkästchen deaktivieren, können Sie ein beliebiges Netzwerk oder einen beliebigen Netzwerkpool auswählen und später ein Organisations-vDC erstellen, das auf diese zugreifen kann.

6 Verwenden Sie die Standardnetzwerkeinstellungen oder geben Sie Ihre eigenen Einstellungen ein und klicken Sie auf **[Weiter]** .

7 (Optional) Geben Sie die externe IP-Adresse zur Verwendung durch die NAT-Dienste ein, klicken Sie auf **[Hinzufügen]** und klicken Sie dann auf **[Weiter]** .

Diese Einstellung ist lediglich in der erweiterten Einrichtung verfügbar. Sie können mehrere externe IP-Adressen hinzufügen.

8 Geben Sie einen Namen und bei Bedarf eine Beschreibung ein und klicken Sie dann auf **[Weiter]** .

9 Überprüfen Sie die Einstellungen für das Organisationsnetzwerk.

Klicken Sie auf **[Fertigstellen]** , um die Einstellungen zu übernehmen und das Organisationsnetzwerk zu erstellen, oder klicken Sie auf **[Zurück]** , um die Einstellungen zu bearbeiten.

Weiter

Wenn Sie externe IP-Adressen hinzugefügt haben, können Sie deren Zuordnung festlegen. Siehe „Konfigurieren der Portweiterleitung für ein Organisationsnetzwerk“, auf Seite 64.

Hinzufügen eines internen Organisationsnetzwerks

Sie können der Umgebung ein internes Organisationsnetzwerk hinzufügen, zu dem mehrere vApps eine Verbindung herstellen können und auf das nur diese Organisation zugreifen kann.

Voraussetzungen

Stellen Sie sicher, dass ein Netzwerkpool vorhanden ist.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationen]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen der Organisation und wählen Sie den Befehl **[Netzwerke hinzufügen]** .

3 Wählen Sie den gewünschten Einrichtungstyp und den Netzwerktyp aus und klicken Sie dann auf **[Weiter]** .

Sie können mit beiden Verfahren ein internes Organisationsnetzwerk erstellen.

Option	Netzwerktyp
Typisch	Aktivieren Sie das Kontrollkästchen für internes Netzwerk.
Erweitert	Wählen Sie die Option **[Internes Organisationsnetzwerk]** .

4 Wählen Sie einen Netzwerkpool aus und klicken Sie dann auf **[Weiter]** .

Wenn Sie das Kontrollkästchen **[Nur Netzwerke verwenden, auf die diese Organisation zugreifen kann]** deaktivieren, werden auch Netzwerkpools angezeigt, die der Organisation aktuell nicht durch ihre Organisations-vDCs verfügbar gemacht wurden. Wenn Sie dieses Kontrollkästchen deaktivieren, können Sie einen beliebigen Netzwerkpool auswählen und später ein Organisations-vDC erstellen, das auf ihn zugreifen kann.

5 Verwenden Sie die Standardnetzwerkeinstellungen oder geben Sie Ihre eigenen Einstellungen ein und klicken Sie auf **[Weiter]** .

6 Geben Sie einen Namen und bei Bedarf eine Beschreibung ein und klicken Sie dann auf **[Weiter]** .

7 Überprüfen Sie die Einstellungen für das Organisationsnetzwerk.

Klicken Sie auf **[Fertigstellen]** , um die Einstellungen zu übernehmen und das Organisationsnetzwerk zu erstellen, oder klicken Sie auf **[Zurück]** , um die Einstellungen zu bearbeiten.

Erstellen eines veröffentlichten Katalogs

4

Sie können einen Katalog veröffentlichen, um eine Zusammenstellung von vApp-Vorlagen oder Mediendateien für alle Organisationen in einer vCloud Director-Installation verfügbar zu machen.

Organisationen verwenden Kataloge, um vApp-Vorlagen und Mediendateien zu speichern. Die Mitglieder einer Organisation können Katalogobjekte als Bausteine zur Erstellung eigener vApps verwenden.

Wenn Sie einen Katalog veröffentlichen, werden die Objekte in dem Katalog allen Organisationen in der vCloud Director-Installation zur Verfügung gestellt. Die Administratoren der einzelnen Organisationen können auswählen, welche Objekte des Katalogs sie für die Benutzer bereitstellen möchten.

Um einen Katalog veröffentlichen zu können, müssen Sie eine Organisation erstellen und bereitstellen, die den Katalog enthält.

Dieses Kapitel behandelt die folgenden Themen:

- „Aktivieren der Katalogveröffentlichung“, auf Seite 37
- „Erstellen eines veröffentlichten Katalogs“, auf Seite 38
- „Hochladen einer vApp-Vorlage“, auf Seite 38
- „Importieren einer vApp-Vorlage aus vSphere“, auf Seite 39
- „Hochladen einer Mediendatei“, auf Seite 39
- „Importieren einer Mediendatei aus vSphere“, auf Seite 40
- „Katalog veröffentlichen“, auf Seite 40

Aktivieren der Katalogveröffentlichung

Sie können den Katalog einer Organisation erst dann veröffentlichen, wenn die Katalogveröffentlichung für die Organisation aktiviert ist.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationen]** .
2. Klicken Sie mit der rechten Maustaste auf den Namen der Organisation und wählen Sie den Befehl **[Eigenschaften]** .
3. Wählen Sie auf der Registerkarte **[Katalogveröffentlichung]** die Option **[Veröffentlichung von Katalogen bei allen Organisationen zulassen]** und klicken Sie auf **[OK]** .

Erstellen eines veröffentlichten Katalogs

Sie können einen veröffentlichten Katalog für die hochgeladenen und importierten vApp-Vorlagen und Mediendateien erstellen, die allen Organisationen zur Verfügung gestellt werden sollen. Organisationen können über mehrere Kataloge verfügen, für die der Zugriff individuell geregelt werden kann.

Voraussetzungen

Prüfen Sie, ob eine Organisation vorhanden ist, die die Katalogveröffentlichung zulässt.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationen]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen der Organisation und wählen Sie den Befehl **[Öffnen]** .

3 Klicken Sie auf **[Kataloge]** und wählen Sie dann im linken Bereich die Option **[Kataloge meiner Organisation]** .

4 Klicken Sie auf der Registerkarte **[Kataloge]** auf **[Neu]** .

5 Geben Sie einen Katalognamen und bei Bedarf eine Beschreibung ein und klicken Sie dann auf **[Weiter]** .

6 Klicken Sie auf **[Weiter]** .

7 Wählen Sie die Option **[Bei allen Organisationen veröffentlichen]** und klicken Sie dann auf **[Weiter]** .

8 Überprüfen Sie die Katalogeinstellungen und klicken Sie auf **[Fertigstellen]** .

Hochladen einer vApp-Vorlage

Sie können ein OVF-Paket als vApp-Vorlage hochladen, um die Vorlage auf diese Weise anderen Benutzern zur Verfügung zu stellen. vCloud Director unterstützt OVF 1.0 und OVF 1.1.

vCloud Director unterstützt OVF-Pakete auf der Basis der OVF (Open Virtualization Format)-Spezifikation. Wenn Sie ein OVF-Paket mit Bereitstellungsoptionen hochladen, bleiben diese Optionen in der vApp-Vorlage erhalten.

Sie können Dateien, die von Benutzern zu vCloud Director hochgeladen werden, unter Quarantäne stellen. So können Sie die Dateien verarbeiten, bevor Sie sie akzeptieren. Sie können die Dateien beispielsweise mit einem Virenscanner überprüfen. Siehe „Quarantäne für hochgeladene Dateien“, auf Seite 120.

Voraussetzungen

Prüfen Sie, ob die folgenden Bedingungen erfüllt sind:

- Die Organisation, in die Sie das OVF-Paket hochladen, hat einen Katalog und ein Organisations-vDC.
- Auf dem Computer, von dem Sie hochladen, ist Java Plug-in 1.6.0_10 oder höher installiert.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationen]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen der Organisation und wählen Sie den Befehl **[Öffnen]** .

3 Klicken Sie auf **[Kataloge]** und wählen Sie dann im linken Bereich die Option **[Kataloge meiner Organisation]** .

4 Klicken Sie auf der Registerkarte **[vApp-Vorlagen]** auf **[Upload]** .

5 Klicken Sie auf **[Durchsuchen]** , navigieren Sie zu dem gewünschten OVF-Paket, wählen Sie es aus und klicken Sie dann auf **[Öffnen]** .

6 Geben Sie einen Namen und bei Bedarf eine Beschreibung für die vApp-Vorlage ein.

7 Wählen Sie ein Organisations-vDC und einen Katalog aus und klicken Sie auf **[Upload]** .

Weiter

Stellen Sie sicher, dass vSphere Tools auf den virtuellen Maschinen in der vApp installiert ist. vSphere Tools wird für die Unterstützung der Gast-Anpassung benötigt. Weitere Informationen erhalten Sie im *VMware vCloud Director-Benutzerhandbuch*.

Importieren einer vApp-Vorlage aus vSphere

Sie können eine virtuelle Maschine aus vSphere importieren und als vApp-Vorlage in einem Katalog speichern, der für andere Benutzer verfügbar ist.

Voraussetzungen

Stellen Sie sicher, dass Sie vCloud Director-Systemadministrator sind.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationen]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen der Organisation und wählen Sie den Befehl **[Öffnen]** .

3 Klicken Sie auf **[Kataloge]** und wählen Sie dann im linken Bereich die Option **[Kataloge meiner Organisation]** .

4 Klicken Sie auf der Registerkarte **[vApp-Vorlagen]** auf **[Von vSphere importieren]** .

5 Wählen Sie einen vCenter Server und eine virtuelle Maschine aus.

6 Geben Sie einen Namen und bei Bedarf eine Beschreibung für die vApp-Vorlage ein.

7 Wählen Sie ein Organisations-vDC und einen Katalog aus.

8 Wählen Sie aus, ob Sie die virtuelle Maschine in den Katalog verschieben oder kopieren möchten.

9 Wählen Sie aus, ob Sie die vApp-Vorlage in dem Katalog als Gold Master kennzeichnen möchten.

Wenn Sie eine vApp-Vorlage als Gold Master kennzeichnen, wird dies in der Liste der vApp-Vorlagen angezeigt.

10 Klicken Sie auf **[OK]** .

Weiter

Überprüfen Sie, ob vSphere Tools auf den virtuellen Maschinen in der vApp installiert ist. vSphere Tools wird für die Unterstützung der Gast-Anpassung benötigt. Weitere Informationen erhalten Sie im *VMware vCloud Director-Benutzerhandbuch*.

Hochladen einer Mediendatei

Sie können eine ISO- oder FLP-Datei hochladen, um auf diese Weise die Medien anderen Benutzern zur Verfügung zu stellen.

Sie können Dateien, die von Benutzern zu vCloud Director hochgeladen werden, unter Quarantäne stellen. So können Sie die Dateien verarbeiten, bevor Sie sie akzeptieren. Sie können die Dateien beispielsweise mit einem Virenscanner überprüfen. Siehe „Quarantäne für hochgeladene Dateien“, auf Seite 120.

Voraussetzungen

Stellen Sie sicher, dass auf dem Computer, von dem Sie hochladen, Java Plug-in 1.6.0_10 oder höher installiert ist.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationen]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen der Organisation und wählen Sie den Befehl **[Öffnen]** .

3 Klicken Sie auf **[Kataloge]** und wählen Sie dann im linken Bereich die Option **[Kataloge meiner Organisation]** .

4 Klicken Sie auf der Registerkarte **[Medien]** auf **[Upload]** .

5 Klicken Sie auf **[Durchsuchen]** , navigieren Sie zu der gewünschten Mediendatei, wählen Sie sie aus und klicken Sie dann auf **[Öffnen]** .

6 Geben Sie einen Namen und bei Bedarf eine Beschreibung für die Mediendatei ein.

7 Wählen Sie ein Organisations-vDC und einen Katalog aus und klicken Sie auf **[Upload]** .

Importieren einer Mediendatei aus vSphere

Sie können Mediendateien aus einem vSphere-Datenspeicher importieren und in einem Katalog speichern, sodass sie für andere Benutzer verfügbar sind.

Voraussetzungen

Sie müssen als Systemadministrator bei vCloud Director angemeldet sein. Sie müssen den Datenspeicher mit der Mediendatei und den Pfad der Datei kennen.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationen]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen der Organisation und wählen Sie den Befehl **[Öffnen]** .

3 Klicken Sie auf **[Kataloge]** und wählen Sie dann im linken Bereich die Option **[Kataloge meiner Organisation]** .

4 Klicken Sie auf der Registerkarte **[Medien]** auf **[Von vSphere importieren]** .

5 Geben Sie einen Namen und bei Bedarf eine Beschreibung für die Mediendatei ein.

6 Wählen Sie den Quell-vCenter Server und den Datenspeicher aus und geben Sie den Pfad zu der Mediendatei ein.

7 Wählen Sie ein Organisations-vDC und einen Katalog aus.

8 Klicken Sie auf **[OK]** .

Katalog veröffentlichen

Sie können einen Katalog veröffentlichen, um die darin enthaltenen vApp-Vorlagen und Mediendateien allen Organisationen in der Installation zur Verfügung zu stellen.

Voraussetzungen

Prüfen Sie, ob die Organisation, die den Katalog enthält, die Katalogveröffentlichung zulässt.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationen]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen der Organisation und wählen Sie den Befehl **[Öffnen]** .

3 Klicken Sie auf **[Kataloge]** und wählen Sie dann im linken Bereich die Option **[Kataloge meiner Organisation]** .

4 Klicken Sie auf der Registerkarte **[Kataloge]** mit der rechten Maustaste auf den Namen des Katalogs und wählen Sie den Befehl **[Veröffentlichen]** .

5 Wählen Sie auf der Registerkarte **[Veröffentlichung]** die Option **[Bei allen Organisationen veröffentlichen]** und klicken Sie auf **[OK]** .

Der Katalog wird mit seinen Inhalten für alle Organisationen in der vCloud Director-Installation unter **[Öffentliche Kataloge]** angezeigt.

Verwalten von Cloud-Ressourcen 5

Provider-vDCs, Organisations-vDCs, externe Netzwerke, Organisationsnetzwerke und Netzwerkpools sind Beispiele für Cloud-Ressourcen. Nachdem Sie vCloud Director Cloud-Ressourcen hinzugefügt haben, können Sie sie bearbeiten und Informationen zu Beziehungen zwischen ihnen anzeigen.

Dieses Kapitel behandelt die folgenden Themen:

- „Verwalten von Provider-vDCs“, auf Seite 43
- „Verwalten von Organisations-vDCs“, auf Seite 48
- „Verwalten externer Netzwerke“, auf Seite 55
- „Verwalten von Organisationsnetzwerken“, auf Seite 56
- „Verwalten von Netzwerkpools“, auf Seite 75
- „Verwalten von Cloud-Zellen“, auf Seite 77

Verwalten von Provider-vDCs

Wenn Sie ein Provider-vDC erstellt haben, können Sie seine Eigenschaften bearbeiten, das vDC deaktivieren oder löschen, sowie seine ESX/ESXi-Hosts und Datenspeicher verwalten.

Aktivieren oder Deaktivieren eines Provider-vDCs

Sie können ein Provider-vDC deaktivieren, um die Erstellung von Organisations-vDCs zu verhindern, die dessen Ressourcen verwenden.

Wenn Sie ein Provider-vDC deaktivieren, deaktiviert vCloud Director auch die Organisations-vDCs, die dessen Ressourcen verwenden. Laufende vApps und eingeschaltete virtuelle Maschinen laufen weiter, aber Sie können weder neue vApps oder virtuelle Maschinen erstellen noch zusätzliche starten.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Provider-vDCs]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des Provider-vDCs und wählen Sie den Befehl **[Aktivieren]** bzw. **[Deaktivieren]** .

Löschen eines Provider-vDCs

Sie können ein Provider-vDC löschen, um seine Rechen-, Arbeitsspeicher- und Speicherressourcen aus vCloud Director zu entfernen. Dieser Vorgang hat in vSphere keine Auswirkungen auf diese Ressourcen.

Voraussetzungen

- Deaktivieren Sie das Provider-vDC.
- Deaktivieren und löschen Sie alle Organisations-vDCs und Organisationsnetzwerke, die das Provider-vDC verwenden.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Provider-vDCs]** .
2. Klicken Sie mit der rechten Maustaste auf den Namen des Provider-vDCs und wählen Sie den Befehl **[Löschen]** .
3. Klicken Sie auf **[Ja]** .

Bearbeiten des Namens und der Beschreibung eines Provider-vDCs

Wenn Ihre vCloud Director-Installation anwächst, besteht möglicherweise Bedarf, einem bestehenden Provider-vDC einen aussagekräftigeren Namen oder eine Beschreibung zuzuweisen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Provider-vDCs]** .
2. Klicken Sie mit der rechten Maustaste auf den Namen des Provider-vDCs und wählen Sie den Befehl **[Eigenschaften]** .
3. Geben Sie einen neuen Namen oder eine neue Beschreibung ein und klicken Sie auf **[OK]** .

   Über den Namen und die Beschreibung können Sie Hinweise zur vSphere-Funktionalität geben, die Provider-vDCs, wie beispielsweise vSphere HA, zur Verfügung gestellt wird.

Aktivieren oder Deaktivieren eines Provider-vDC-Hosts

Sie können einen Host deaktivieren, um zu verhindern, dass auf dem Host vApps gestartet werden. Virtuelle Maschinen, die zu diesem Zeitpunkt bereits auf dem Host ausgeführt werden, sind nicht betroffen.

Wenn Sie an einem Host Wartungen durchführen müssen, migrieren Sie alle vApps zu einem anderen Host und deaktivieren Sie dann den ersten Host.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Provider-vDCs]** .
2. Klicken Sie mit der rechten Maustaste auf den Namen des Provider-vDCs und wählen Sie den Befehl **[Öffnen]** .
3. Klicken Sie auf die Registerkarte **[Hosts]** .
4. Klicken Sie mit der rechten Maustaste auf den Namen des Hosts und wählen Sie den Befehl **[Host aktivieren]** bzw. **[Host deaktivieren]** .

vCloud Director aktiviert bzw. deaktiviert den Host für alle Provider-vDCs, die dessen Ressourcen verwenden.

Vorbereiten eines Provider-vDC-Hosts und Rückgängigmachen der Vorbereitung

Wenn Sie einem vSphere-Cluster, der von vCloud Director verwendet wird, einen ESX/ESXi-Host hinzufügen, müssen Sie den Host vorbereiten, bevor Provider-vDCs seine Ressourcen nutzen können. Sie können die Vorbereitung eines Hosts auch rückgängig machen, um ihn aus der vCloud Director-Umgebung zu entfernen.

Informationen zum Verschieben von bereits ausgeführten virtuellen Maschinen zwischen Hosts erhalten Sie unter „Verschieben von virtuellen Maschinen zwischen ESX/ESXi-Hosts“, auf Seite 82.

Hosts, die sich im gesperrten Modus befinden, können nicht vorbereitet werden. Nach dem Vorbereiten eines Hosts kann er in den gesperrten Modus versetzt werden.

Voraussetzungen

Wenn Sie die Vorbereitung eines Hosts rückgängig machen möchten, müssen Sie ihn zunächst deaktivieren, um sicherzustellen, dass auf dem Host keine virtuellen Maschinen mehr ausgeführt werden.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Provider-vDCs]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des Provider-vDCs und wählen Sie den Befehl **[Öffnen]** .

3 Klicken Sie auf die Registerkarte **[Hosts]** .

4 Klicken Sie mit der rechten Maustaste auf den Namen des Hosts und wählen Sie den Befehl **[Host vorbereiten]** bzw. **[Vorbereitung für Host rückgängig]** .

vCloud Director bereitet den Host für alle Provider-vDCs vor, die dessen Ressourcen verwenden, bzw. macht die Vorbereitung rückgängig.

Aktualisieren eines ESX/ESXi-Host-Agenten für einen Provider-vDC-Host

vCloud Director installiert die Agent-Software auf allen ESX/ESXi-Hosts in der Installation. Wenn Sie Ihre ESX/ESXi-Hosts aktualisieren, müssen Sie gleichzeitig auch Ihre ESX/ESXi-Host-Agents aktualisieren.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Provider-vDCs]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des Provider-vDCs und wählen Sie den Befehl **[Öffnen]** .

3 Klicken Sie auf die Registerkarte **[Hosts]** .

4 Klicken Sie mit der rechten Maustaste auf den Benutzernamen und wählen Sie den Befehl **[Host-Agent-Upgrade]** .

vCloud Director aktualisiert den Host-Agent. Die Aktualisierung betrifft alle Provider-vDCs, die den Host verwenden.

Reparieren eines Provider-vDC-ESX/ESXi-Hosts

Wenn auf einem ESX/ESXi-Host der vCloud Director-Agent nicht mehr antwortet, versuchen Sie, den Host zu reparieren.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Provider-vDCs]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des Provider-vDCs und wählen Sie den Befehl **[Öffnen]** .

3 Klicken Sie auf die Registerkarte **[Hosts]** .

4 Klicken Sie mit der rechten Maustaste auf den Benutzernamen und wählen Sie den Befehl **[Host reparieren]** .

vCloud Director repariert den Host. Der Vorgang betrifft alle Provider-vDCs, die den Host verwenden.

Aktivieren oder Deaktivieren eines Provider-vDC-Datenspeichers

Wenn Sie einen Datenspeicher deaktivieren, können diesem Datenspeicher zugeordnete vApps nicht mehr gestartet werden, und es können keine vApps auf dem Datenspeicher mehr erstellt werden.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Provider-vDCs]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des Provider-vDCs und wählen Sie den Befehl **[Öffnen]** .

3 Klicken Sie auf die Registerkarte **[Datenspeicher]** .

4 Klicken Sie mit der rechten Maustaste auf den Namen des Datenspeichers und wählen Sie den Befehl **[Aktivieren]** bzw. **[Deaktivieren]** .

vCloud Director aktiviert bzw. deaktiviert den Datenspeicher für alle Provider-vDCs, die dessen Ressourcen verwenden.

Hinzufügen von Speicherkapazität zu einem Provider-vDC

Sie können einem Provider-vDC Speicherkapazität hinzufügen, indem Sie einen oder mehrere Datenspeicher hinzufügen.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Provider-vDCs]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des Provider-vDCs und wählen Sie den Befehl **[Öffnen]** .

3 Klicken Sie auf die Registerkarte **[Datenspeicher]** .

4 Klicken Sie auf **[Hinzufügen/entfernen]** .

5 Wählen Sie einen Datenspeicher aus, klicken Sie auf **[Hinzufügen]** und klicken Sie dann auf **[OK]** .

   vCloud Director unterstützt bei Provider-vDCs nicht die Verwendung von schreibgeschützten Datenspeichern. In der Regel werden schreibgeschützte Datenspeicher nicht in der Liste aufgeführt, aber einige schreibgeschützte NFS-Datenspeicher können angezeigt werden. Fügen Sie diese Datenspeicher dem Provider-vDC nicht hinzu.

   Verwenden Sie nur gemeinsam genutzten Speicher, da vSphere DRS die Migration von virtuellen Maschinen im lokalen Speicher nicht unterstützt.

vCloud Director fügt dem Provider-vDC den Datenspeicher hinzu.

Hinzufügen eines Ressourcenpools zu einem Provider-vDC

Sie haben die Möglichkeit, einem Provider-vDC zusätzliche Ressourcenpools hinzuzufügen, damit vom Provider-vDC bereitgestellte Pay-As-You-Go-Organisations-vDCs erweitert werden können.

Wenn Rechenressourcen von mehreren Ressourcenpools gestützt werden, können sie nach Bedarf für weitere virtuelle Maschinen erweitert werden.

Voraussetzungen

Stellen Sie sicher, dass in dem vCenter-Datencenter, in dem sich der primäre Ressourcenpol des Provider-vDCs befindet, mindestens ein verfügbarer Ressourcenpool vorhanden ist.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Provider-vDCs]** .
2. Klicken Sie mit der rechten Maustaste auf den Namen des Provider-vDCs und wählen Sie den Befehl **[Öffnen]** .
3. Klicken Sie auf die Registerkarte **[Ressourcenpools]** .
4. Klicken Sie auf **[Ressourcenpool hinzufügen]** .
5. Wählen Sie den Ressourcenpool aus, der hinzugefügt werden soll, und klicken Sie auf **[Fertigstellen]** .

vCloud Director fügt einen Ressourcenpool hinzu, der vom Provider-vDC verwendet werden soll, sodass alle von diesem Provider-vDC gestützten Pay-As-You-Go-Organisations-vDCs elastisch werden.

Konfigurieren der Warnmeldungen über zu niedrige verbleibende Festplattenkapazität für einen Provider-vDC-Datenspeicher

Sie können Warnmeldungen über zu niedrige verbleibende Festplattenkapazität auf einem Datenspeicher so konfigurieren, dass vCloud Director mit dem Erreichen eines bestimmten Schwellenwertes zur verfügbaren Kapazität eine entsprechende Warnmeldung per E-Mail versendet. Diese E-Mail-Nachricht dient dazu, Sie von der Situation des geringen verbleibenden Speicherplatzes in Kenntnis zu setzen, bevor dies problematisch werden könnte.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Provider-vDCs]** .
2. Klicken Sie mit der rechten Maustaste auf den Namen des Provider-vDCs und wählen Sie den Befehl **[Öffnen]** .
3. Klicken Sie auf die Registerkarte **[Datenspeicher]** .
4. Klicken Sie mit der rechten Maustaste auf den Namen des Datenspeichers und wählen Sie den Befehl **[Eigenschaften]** .
5. Wählen Sie die Festplattenkapazität-Schwellenwerte für den Datenspeicher aus.

   Sie können zwei Schwellenwerte festlegen, einen gelben und einen roten. Wenn vCloud Director eine Warnmeldung per E-Mail versendet, wird auf dieser Nachricht vermerkt, welcher der beiden Schwellenwerte unterschritten wurde.
6. Klicken Sie auf **[OK]** .

vCloud Director legt Schwellenwerte für alle Provider-vDCs fest, die den Datenspeicher verwenden. vCloud Director versendet eine Warnmeldung per E-Mail, wenn ein Datenspeicher den Schwellenwert unterschreitet.

Versenden einer E-Mail-Benachrichtigung an Provider-vDC-Benutzer

Sie können allen Benutzern, denen Objekte im Provider-vDC, z. B. vApps oder Mediendateien, gehören, eine E-Mail-Benachrichtigung senden. Mit einer E-Mail-Benachrichtigung können Sie beispielsweise Benutzer über geplante Systemwartungen in Kenntnis setzen.

Voraussetzungen

Überprüfen Sie, ob eine gültige Verbindung zu einem SMTP-Server besteht.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Provider-vDCs]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des Provider-vDCs und wählen Sie den Befehl **[Benachrichtigen]** .

3 Geben Sie den Betreff und den Nachrichtentext ein und klicken Sie auf **[E-Mail senden]** .

Verwalten von Organisations-vDCs

Wenn Sie ein Organisations-vDC erstellt haben, können Sie seine Eigenschaften bearbeiten, das vDC deaktivieren oder löschen, sowie sein Zuweisungsmodell, den Speicher und die Netzwerkeinstellungen verwalten.

Erstellen eines Organisations-vDC

Erstellen Sie ein Organisations-vDC, um einer Organisation Ressourcen zuzuweisen. Organisations-vDCs werden von einem Provider-vDC abgetrennt. Jede Organisation kann über mehrere Organisations-vDCs verfügen.

Voraussetzungen

Sie können Organisationen erst dann Ressourcen zuweisen, wenn ein Provider-vDC eingerichtet ist.

Vorgehensweise

1 Öffnen des Assistenten für neue Organisations-vDCs auf Seite 49

Öffnen Sie den Assistenten für neue Organisations-vDCs, um den Vorgang zum Erstellen eines Organisations-vDC zu starten.

2 Auswählen einer Organisation für das Organisations-vDC auf Seite 49

Sie können ein Organisations-vDC erstellen, das Ressourcen für beliebige Organisationen in dem vCloud Director-System bereitstellen kann. Organisationen können über mehrere Organisations-vDC verfügen.

3 Auswählen eines Provider-vDC auf Seite 49

Organisations-vDCs erhalten ihre Rechen- und Arbeitsspeicherressourcen von einem Provider-vDC. Das Organisations-vDC stellt diese Ressourcen vApps und virtuellen Maschinen in der Organisation zur Verfügung.

4 Auswählen eines Zuweisungsmodells auf Seite 50

Über das Zuweisungsmodell wird festgelegt, auf welche Weise und zu welchem Zeitpunkt das Provider-vDC die von Ihnen zugewiesenen Rechen- und Arbeitsspeicherressourcen den Organisations-vDCs zusichert.

5 Konfigurieren des Zuweisungsmodells auf Seite 50

Sie konfigurieren das Zuweisungsmodell, indem Sie eine Menge von Provider-vDC-Ressourcen angeben, die dem Organisations-vDC zugewiesen werden soll.

6 Zuweisen von Speicher auf Seite 51

Organisations-vDCs benötigen Speicherplatz für vApps und vApp-Vorlagen. Sie können Speicher zuweisen, der über die Provider-vDC-Datenspeicher zur Verfügung steht.

7 Auswählen eines Netzwerkpools auf Seite 52

Bei einem Netzwerkpool handelt es sich um eine Gruppe undifferenzierter Netzwerke, die zur Erstellung von vApp-Netzwerken und NAT-geleiteten oder internen Organisationsnetzwerken verwendet werden.

8 Festlegen eines Namens für das Organisations-vDC auf Seite 52

Sie können einen beschreibenden Namen und eine optionale Beschreibung bereitstellen, um die für das neue Organisations-vDC verfügbaren vSphere-Funktionen anzugeben.

9 Bestätigen der Einstellungen und Erstellen des Organisations-vDCs auf Seite 52

Überprüfen Sie die eingegebenen Einstellungen, bevor Sie das neue Organisations-vDC erstellen.

Öffnen des Assistenten für neue Organisations-vDCs

Öffnen Sie den Assistenten für neue Organisations-vDCs, um den Vorgang zum Erstellen eines Organisations-vDC zu starten.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisations-vDC]** .

2 Klicken Sie auf die Schaltfläche **[Neues vDC]** .

Auswählen einer Organisation für das Organisations-vDC

Sie können ein Organisations-vDC erstellen, das Ressourcen für beliebige Organisationen in dem vCloud Director-System bereitstellen kann. Organisationen können über mehrere Organisations-vDC verfügen.

Vorgehensweise

1 Wählen Sie eine Organisation aus.

2 Klicken Sie auf **[Weiter]** .

Auswählen eines Provider-vDC

Organisations-vDCs erhalten ihre Rechen- und Arbeitsspeicherressourcen von einem Provider-vDC. Das Organisations-vDC stellt diese Ressourcen vApps und virtuellen Maschinen in der Organisation zur Verfügung.

Vorgehensweise

1 Wählen Sie ein Provider-vDC aus.

In der Liste der Provider-vDCs werden Informationen zu verfügbaren Ressourcen und in der Netzwerkliste für das ausgewählte Provider-vDC Informationen zu verfügbaren Netzwerken angezeigt.

2 Klicken Sie auf **[Weiter]** .

Auswählen eines Zuweisungsmodells

Über das Zuweisungsmodell wird festgelegt, auf welche Weise und zu welchem Zeitpunkt das Provider-vDC die von Ihnen zugewiesenen Rechen- und Arbeitsspeicherressourcen den Organisations-vDCs zusichert.

Vorgehensweise

1 Wählen Sie ein Zuweisungsmodell aus.

Option	Beschreibung
Zuweisungspool	Nur ein Teil der von Ihnen zugewiesenen Ressourcen wird dem Organisations-vDC zugesichert. Sie können Ressourcen überbelegen, indem Sie den Prozentsatz angeben.
Pay-As-You-Go	Ressourcen werden erst zugesichert, wenn Benutzer in dem Organisations-vDC vApps erstellen. Sie können Ressourcen überbelegen, indem Sie den Prozentsatz der garantierten Ressourcen angeben. Sie können ein Pay-As-You-Go-Organisations-vDC „elastisch“ machen, indem Sie mehrere Ressourcenpools zu seinem Provider-vDC hinzufügen.
Reservierungspool	Alle von Ihnen zugewiesenen Ressourcen werden dem Organisations-vDC sofort zugesichert. Die Benutzer in der Organisation können die Überbelegung steuern, indem sie Reservierungs-, Grenzwert- und Prioritätseinstellungen für einzelne virtuelle Maschinen festlegen.

2 Klicken Sie auf **[Weiter]** .

Konfigurieren des Zuweisungsmodells

Sie konfigurieren das Zuweisungsmodell, indem Sie eine Menge von Provider-vDC-Ressourcen angeben, die dem Organisations-vDC zugewiesen werden soll.

Vorgehensweise

1 Wählen Sie die Optionen für Zuweisungsmodelle aus.

Es sind nicht für jedes Modell alle Optionen verfügbar.

Option	Aktion
CPU-Zuweisung	Geben Sie die maximale Menge an Prozessorleistung in GHz an, die den virtuellen Maschinen in dem Organisations-vDC zugewiesen werden soll.
Garantierte CPU-Ressourcen	Geben Sie den Prozentsatz der Prozessorleistung an, die den virtuellen Maschinen in dem Organisations-vDC garantiert werden soll. Sie können Ressourcen überbelegen, indem Sie weniger als 100 % garantieren.
Arbeitsspeicherzuweisung	Geben Sie die maximale Arbeitsspeichermenge in GB an, die den virtuellen Maschinen in dem Organisations-vDC zugewiesen werden soll.
Garantierte Arbeitsspeicherressourcen	Geben Sie den Prozentsatz des Arbeitsspeichers an, der den virtuellen Maschinen in dem Organisations-vDC garantiert werden soll. Sie können Ressourcen überbelegen, indem Sie weniger als 100 % garantieren.
vCPU-Geschwindigkeit	Geben Sie die vCPU-Geschwindigkeit in GHz ein. Anschließend wird den virtuellen Maschinen in dem Organisations-vDC dieser Wert in GHz pro vCPU zugewiesen.
Maximale Anzahl der VMs	Geben Sie die maximale Anzahl virtueller Maschinen an, die in diesem Organisations-vDC erstellt werden dürfen.

2 Klicken Sie auf **[Weiter]** .

Beispiel: Konfigurieren eines Zuweisungsmodells

Wenn Sie ein Organisations-vDC anlegen, erstellt vCloud Director auf der Basis der festgelegten Einstellungen des Zuweisungsmodells einen vSphere-Ressourcenpool. Siehe Tabelle 5-1, Tabelle 5-2 und Tabelle 5-3.

Tabelle 5-1. Auswirkungen der Einstellungen für den Zuweisungspool auf die Einstellungen für den Ressourcenpool

Zuweisungspooleinstellung	Zuweisungspoolwert	Ressourcenpooleinstellung	Ressourcenpoolwert
CPU-Zuweisung	25 GHz	CPU-Limit	25 GHz
CPU % garantiert	10 %	CPU-Reservierung	2,5 GHz
Arbeitsspeicherzuweisung	50 GB	Arbeitsspeicher-Limit	50 GB
Arbeitsspeicher % garantiert	20 %	Arbeitsspeicherreservierung	10 GB

Tabelle 5-2. Auswirkungen der Pay-As-You-Go-Einstellungen auf die Einstellungen für den Ressourcenpool

Pay-As-You-Go-Einstellung	Pay-As-You-Go-Wert	Ressourcenpooleinstellung	Ressourcenpoolwert
CPU % garantiert	10 %	CPU-Reservierung, CPU-Limit	0,00 GHz, Unbegrenzt
Arbeitsspeicher % garantiert	100 %	Arbeitsspeicherreservierung, Arbeitsspeicher-Limit	0,00 GB, Unbegrenzt

Für Ressourcenpools, die Pay-As-You-Go-Organisations-vDCs unterstützen, können weder Reservierungen noch Grenzwerte angegeben werden. Pay-As-You-Go-Einstellungen betreffen ausschließlich die Überbelegung. Eine Garantie von 100 % bedeutet, dass keine Überbelegung möglich ist. Je niedriger der Prozentsatz, desto mehr Überbelegung ist möglich.

Tabelle 5-3. Auswirkungen der Einstellungen für den Reservierungspool auf die Einstellungen für den Ressourcenpool

Reservierungspooleinstellung	Reservierungspoolwert	Ressourcenpooleinstellung	Ressourcenpoolwert
CPU-Zuweisung	25 GHz	CPU-Reservierung, CPU-Limit	25 GHz, 25 GHz
Arbeitsspeicherzuweisung	50 GB	Arbeitsspeicherreservierung, Arbeitsspeicher-Limit	50 GB, 50 GB

Zuweisen von Speicher

Organisations-vDCs benötigen Speicherplatz für vApps und vApp-Vorlagen. Sie können Speicher zuweisen, der über die Provider-vDC-Datenspeicher zur Verfügung steht.

Durch den Einsatz von Thin Provisioning kann die Zuweisung von übermäßigem Speicher vermieden werden, und generell kann Speicherplatz gespart werden. Für eine virtuelle Maschine mit einer „schlanken“ virtuellen Festplatte stellt ESX/ESXi den gesamten Speicherplatz bereit, der für aktuelle und künftige Operationen der Festplatte benötigt wird. ESX/ESXi übergibt jedoch nur so viel Speicherplatz, wie die Festplatte für den anfänglichen Betrieb benötigt.

Bei Fast Provisioning wird dadurch Zeit eingespart, dass für bestimmte Operationen von vSphere untereinander verbundene Klone verwendet werden. Weitere Informationen erhalten Sie unter „Fast Provisioning virtueller Maschinen“, auf Seite 95.

Wichtig Fast Provisioning erfordert vCenter Server 5.0 und ESXi 5.0-Hosts. Wenn das Provider-vDC, auf dem das Organisations-vDC basiert, ESX/ESXi 4.x-Hosts enthält, müssen Sie Fast Provisioning deaktivieren. Wenn das Provider-vDC, auf dem das Organisations-vDC basiert, mit mehr als acht Hosts verbundene VMFS-Datenspeicher enthält, kann das Einschalten von virtuellen Maschinen fehlschlagen. Stellen Sie sicher, dass die Datenspeicher mit maximal acht Hosts verbunden sind.

Vorgehensweise

1 Geben Sie das zuzuweisende Speichervolumen ein.

2 (Optional) Mit dem Kontrollkästchen **[Thin Provisioning aktivieren]** können Sie die „schlanke Speicherzuweisung“ für virtuelle Maschinen in dem Organisations-vDC aktivieren.

3 (Optional) Mit dem Kontrollkästchen **[Fast Provisioning aktivieren]** können Sie die „schnelle Bereitstellung“ für virtuelle Maschinen in dem Organisations-vDC deaktivieren.

4 Klicken Sie auf **[Weiter]** .

Auswählen eines Netzwerkpools

Bei einem Netzwerkpool handelt es sich um eine Gruppe undifferenzierter Netzwerke, die zur Erstellung von vApp-Netzwerken und NAT-geleiteten oder internen Organisationsnetzwerken verwendet werden.

Vorgehensweise

1 Wählen Sie einen Netzwerkpool aus oder wählen Sie die Option **[Keine]** .

Wenn Sie die Option **[Keine]** wählen, können Sie zu einem späteren Zeitpunkt einen Netzwerkpool hinzufügen.

2 Geben Sie die maximale Anzahl an Netzwerken ein, die die Organisation aus dem Netzwerkpool bereitstellen kann.

3 Klicken Sie auf **[Weiter]** .

Festlegen eines Namens für das Organisations-vDC

Sie können einen beschreibenden Namen und eine optionale Beschreibung bereitstellen, um die für das neue Organisations-vDC verfügbaren vSphere-Funktionen anzugeben.

Vorgehensweise

1 Geben Sie einen Namen und bei Bedarf eine Beschreibung ein.

2 Klicken Sie auf **[Weiter]** .

Bestätigen der Einstellungen und Erstellen des Organisations-vDCs

Überprüfen Sie die eingegebenen Einstellungen, bevor Sie das neue Organisations-vDC erstellen.

Vorgehensweise

1 Überprüfen Sie die Einstellungen für das Organisations-vDC.

2 (Optional) Klicken Sie auf **[Zurück]** , wenn Sie die Einstellungen ändern möchten.

3 Klicken Sie auf **[Fertigstellen]** , um die Einstellungen zu übernehmen und das Organisations-vDC zu erstellen.

Wenn Sie ein Organisations-vDC anlegen, erstellt vCloud Director in vSphere einen Ressourcenpool, über den Prozessor- und Arbeitsspeicherressourcen bereitgestellt werden.

Aktivieren oder Deaktivieren eines Organisations-vDCs

Sie können ein Organisations-vDC deaktivieren, um zu verhindern, dass die Rechen- und Speicherressourcen des vDCs durch andere vApps und virtuelle Maschinen genutzt werden. Laufende vApps und eingeschaltete virtuelle Maschinen laufen weiter, aber Sie können weder neue vApps oder virtuelle Maschinen erstellen noch zusätzliche starten.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisations-vDCs]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des Organisations-vDCs und wählen Sie den Befehl **[Aktivieren]** bzw. **[Deaktivieren]** .

Löschen eines Organisations-vDCs

Sie können ein Organisations-vDC löschen, um seine Rechen-, Arbeitsspeicher- und Speicherressourcen aus der Organisation zu entfernen. Dieser Vorgang hat in dem Quell-Provider-vDC keine Auswirkungen auf diese Ressourcen.

Voraussetzungen

Deaktivieren Sie das Organisations-vDC und verschieben oder löschen Sie seine vApps, vApp-Vorlagen und Medien.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisations-vDCs]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des Organisations-vDCs und wählen Sie den Befehl **[Löschen]** .

3 Klicken Sie auf **[Ja]** .

Bearbeiten des Namens und der Beschreibung eines Organisations-vDCs

Wenn Ihre vCloud Director-Installation anwächst, besteht möglicherweise Bedarf, einem bestehenden Organisations-vDC einen aussagekräftigeren Namen oder eine Beschreibung zuzuweisen.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisations-vDCs]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des Organisations-vDCs und wählen Sie den Befehl **[Eigenschaften]** .

3 Geben Sie auf der Registerkarte **[Allgemein]** einen neuen Namen bzw. eine neue Beschreibung ein und klicken Sie auf **[OK]** .

Über den Namen und die Beschreibung können Sie Hinweise zu den vSphere-Funktionen geben, die Organisations-vDCs, wie beispielsweise vSphere HA, zur Verfügung gestellt werden.

Bearbeiten der Einstellungen von Zuweisungsmodellen für Organisations-vDCs

Sie können nicht das Zuweisungsmodell von Organisations-vDCs ändern, jedoch können Sie bestimmte Einstellungen des Zuweisungsmodells, das beim Erstellen des Organisations-vDCs festgelegt wurde, ändern.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisations-vDC]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des Organisations-vDCs und wählen Sie den Befehl **[Eigenschaften]** .

3 Geben Sie in der Registerkarte **[Zuweisung]** die neuen Zuweisungsmodelleinstellungen ein und klicken Sie dann auf **[OK]** .

Die Einstellungen gelten nur für vApps, die nach dem Zeitpunkt der Änderung gestartet werden. vApps, die zu diesem Zeitpunkt bereits ausgeführt werden, sind nicht betroffen. Die Informationen zur Nutzung bzw. Auslastung, die vCloud Director für dieses Organisations-vDC berichtet, werden erst dann auf der Grundlage der neuen Einstellungen erstellt, wenn alle ausgeführten vApps angehalten und neu gestartet werden.

Bearbeiten der Speichereinstellungen von Organisations-vDCs

Möglicherweise möchten Sie erstellten Organisations-vDCs, die bereits in Betrieb sind, nachträglich zusätzliche Speicherressourcen aus dem zugehörigen Provider-vDC zur Verfügung stellen. Darüber hinaus können Sie die schlanke Bereitstellung („Thin Provisioning“) bzw. schnelle Bereitstellung („Fast Provisioning“) für das Organisations-vDC aktivieren bzw. deaktivieren.

Informationen zu Fast Provisioning erhalten Sie unter „Fast Provisioning virtueller Maschinen“, auf Seite 95.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisations-vDCs]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des Organisations-vDC und wählen Sie den Befehl **[Eigenschaften]** .

3 Geben Sie auf der Registerkarte **[Speicher]** die neuen Speichereinstellungen ein und klicken Sie dann auf **[OK]** .

WICHTIG Fast Provisioning erfordert vCenter Server 5.0 und ESXi 5.0-Hosts. Wenn das Provider-vDC, auf dem das Organisations-vDC basiert, ESX/ESXi 4.x-Hosts enthält, müssen Sie Fast Provisioning deaktivieren.

Bearbeiten der Netzwerkeinstellungen von Organisations-vDCs

Sie können die maximale Anzahl an bereitgestellten Netzwerken in einem Organisations-vDC und den Netzwerkpool, von dem aus die Netzwerke bereitgestellt werden, ändern.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisations-vDC]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des Organisations-vDCs und wählen Sie den Befehl **[Eigenschaften]** .

3 Geben Sie auf der Registerkarte **[Netzwerkpool]** die neuen Netzwerkeinstellungen ein und klicken Sie dann auf **[OK]** .

Verwalten externer Netzwerke

Wenn Sie ein externes Netzwerk erstellt haben, können Sie seinen Namen, seine Beschreibung und seine Netzwerkspezifikation bearbeiten, seinem IP-Adresspool IP-Adressen hinzufügen und das Netzwerk löschen.

Bearbeiten des Netzwerknamens und der Beschreibung eines externen Netzwerks

Wenn Ihre vCloud Director-Installation anwächst, besteht möglicherweise Bedarf, einem bestehenden externen Netzwerk einen aussagekräftigeren Namen oder eine Beschreibung zuzuweisen.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Externe Netzwerke]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des externen Netzwerks und wählen Sie den Befehl **[Eigenschaften]** .

3 Geben Sie auf der Registerkarte **[Name und Beschreibung]** einen neuen Namen und eine neue Beschreibung ein und klicken Sie auf **[OK]** .

Bearbeiten der Spezifikation eines externen Netzwerks

Wenn sich bei externen Netzwerken die Netzwerkspezifikation ändert, können Sie deren Netzwerkeinstellungen ändern.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Externe Netzwerke]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des externen Netzwerks und wählen Sie den Befehl **[Eigenschaften]** .

3 Bearbeiten Sie auf der Registerkarte **[Netzwerkspezifikation]** die Netzwerkeinstellungen und klicken Sie auf **[OK]** .

Die Netzwerkmaske und das Standard-Gateway können nicht geändert werden. Wenn Sie ein externes Netzwerk mit einer anderen Netzwerkmaske oder einem anderen Gateway benötigen, erstellen Sie ein neues.

Hinzufügen von IP-Adressen zu dem IP-Pool eines externen Netzwerks

Wenn in einem externen Netzwerk nicht mehr genügend IP-Adressen verfügbar sind, können Sie dem zugehörigen IP-Pool weitere IP-Adressen hinzufügen.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Externe Netzwerke]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des externen Netzwerks und wählen Sie den Befehl **[Eigenschaften]** .

3 Geben Sie auf der Registerkarte **[Netzwerkspezifikation]** eine IP-Adresse oder einen Bereich von IP-Adressen in das Textfeld ein, und klicken Sie auf **[Hinzufügen]** .

4 Klicken Sie auf **[OK]** .

Löschen eines externen Netzwerks

Löschen Sie ein externes Netzwerk, um es aus vCloud Director zu entfernen.

Voraussetzungen

Sie können ein externes Netzwerk erst dann löschen, wenn Sie alle Organisationsnetzwerke gelöscht haben, die von ihm abhängig sind.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Externe Netzwerke]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des externen Netzwerks und wählen Sie den Befehl **[Netzwerk löschen]** .

Verwalten von Organisationsnetzwerken

Die Berechtigung zum Hinzufügen, Zurücksetzen und Löschen von Organisationsnetzwerken ist Systemadministratoren vorbehalten.

Systemadministratoren und Organisationsadministratoren können die Eigenschaften von Organisationsnetzwerken bearbeiten, Dienste von Organisationsnetzwerken konfigurieren und IP-Adresszuweisungen anzeigen.

Erstellen von Organisationsnetzwerken

Fügen Sie Ihrer Organisation ein Netzwerk hinzu, über das die virtuellen Maschinen miteinander Daten austauschen können und über das ein Internetzugang bereitgestellt werden kann. Jede Organisation kann über mehrere Organisationsnetzwerke verfügen.

Tabelle 5-4 enthält eine Beschreibung der Arten von Organisationsnetzwerken.

Tabelle 5-4. Arten von Organisationsnetzwerken und ihre Voraussetzungen

Organisationsnetzwerk-typ	Beschreibung	Voraussetzungen
Externes Organisationsnetzwerk – direkte Verbindung	Ermöglicht den Zugriff durch mehrere Organisationen. Zu verschiedenen Organisationen gehörende VMs können sich mit diesem Netzwerk verbinden und den Datenverkehr dieses Netzwerkes sehen. Dieses Netzwerk stellt die direkte Layer-2-Konnektivität für Rechner außerhalb der Organisation zur Verfügung. Computer außerhalb dieser Organisation können direkt eine Verbindung zu den Computern in der Organisation herstellen.	Externes Netzwerk
Externes Organisationsnetzwerk – Verbindung mit NAT-Routing	Ermöglicht den Zugriff nur durch diese Organisation. Nur virtuelle Maschinen in dieser Organisation können sich mit diesem Netzwerk verbinden. Dieses Netzwerk bietet auch den kontrollierten Zugriff auf ein externes Netzwerk. Die System- und Organisationsadministratoren können das NAT-Modul und die Firewall-Einstellungen so konfigurieren, dass der Zugriff vom externen Netzwerk auf ausgewählte virtuelle Maschinen ermöglicht wird.	Externes Netzwerk und Netzwerkpool
Internes Organisationsnetzwerk	Ermöglicht den Zugriff nur durch diese Organisation. Nur virtuelle Maschinen in dieser Organisation können sich mit diesem Netzwerk verbinden und den Datenverkehr in diesem Netzwerk sehen. Dieses Netzwerk stellt ein isoliertes, privates Netzwerk für eine Organisation bereit, mit dem sich mehrere vApps verbinden können. Dieses Netzwerk bietet keine Konnektivität für Rechner außerhalb dieser Organisation. Computer außerhalb dieser Organisation können keine Verbindung zu den Computern in der Organisation herstellen.	Netzwerkpool

Erstellen eines externen direkten Organisationsnetzwerks

Sie können ein externes direktes Organisationsnetzwerk erstellen, auf das mehrere Organisationen zugreifen können. Sie stellen normalerweise über das externe Netzwerk eine Verbindung zum Internet her. Die Organisation stellt die Verbindung zu diesem Netzwerk direkt her.

Voraussetzungen

Ein externes Netzwerk.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationsnetzwerke]** .

2 Klicken Sie auf **[Netzwerk hinzufügen]** .

Der Assistent zur Erstellung von Organisationsnetzwerken wird gestartet.

3 Wählen Sie eine Organisation aus und klicken Sie dann auf **[Weiter]** .

4 Wählen Sie den gewünschten Einrichtungstyp und den Netzwerktyp aus und klicken Sie dann auf **[Weiter]** .

Sie können beide Verfahren verwenden, um ein externes, direktes Organisationsnetzwerk zu erstellen.

Option	Netzwerktyp
Typisch	Aktivieren Sie das Kontrollkästchen für das externe Netzwerk und wählen Sie aus dem Dropdown-Menü die Option **[Direkte Verbindung]** .
Erweitert	Wählen Sie die Option **[Externes Organisationsnetzwerk – direkte Verbindung]** .

5 Wählen Sie ein externes Netzwerk aus und klicken Sie dann auf **[Weiter]** .

Wenn Sie das Kontrollkästchen **[Nur Netzwerke verwenden, auf die diese Organisation zugreifen kann]** deaktivieren, werden auch externe Netzwerke angezeigt, die der Organisation aktuell nicht durch ihre Organisations-vDCs verfügbar gemacht wurden. Wenn Sie dieses Kontrollkästchen deaktivieren, können Sie ein beliebiges Netzwerk auswählen und später ein Organisations-vDC erstellen, das auf das Netzwerk zugreifen kann.

6 Geben Sie einen Namen und bei Bedarf eine Beschreibung ein und klicken Sie dann auf **[Weiter]** .

7 Überprüfen Sie die Einstellungen für das Organisationsnetzwerk.

Klicken Sie auf **[Fertigstellen]** , um die Einstellungen zu übernehmen und das Organisationsnetzwerk zu erstellen, oder klicken Sie auf **[Zurück]** , um die Einstellungen zu bearbeiten.

Erstellen eines externen Organisationsnetzwerks mit NAT-Routing

Sie können ein externes Organisationsnetzwerk mit NAT-Routing erstellen, für das der Zugriff auf diese Organisation eingeschränkt ist. Ein externes Organisationsnetzwerk mit NAT-Routing bietet Geräten außerhalb der Organisation NAT-Konnektivität, wodurch die Kontrollmöglichkeiten der Zugriffsberechtigungen verbessert werden.

Voraussetzungen

Stellen Sie sicher, dass Ihre Organisation über ein externes Netzwerk und einen Netzwerkpool verfügt.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationsnetzwerke]** .

2 Klicken Sie auf **[Netzwerk hinzufügen]** .

Der Assistent zur Erstellung von Organisationsnetzwerken wird gestartet.

3 Wählen Sie eine Organisation aus und klicken Sie dann auf **[Weiter]** .

4 Wählen Sie den gewünschten Einrichtungstyp und den Netzwerktyp aus und klicken Sie dann auf **[Weiter]** .

Sie können beide Verfahren verwenden, um ein externes Organisationsnetzwerk mit Routing zu erstellen.

Option	Netzwerktyp
Typisch	Aktivieren Sie das Kontrollkästchen **[Externes Netzwerk]** und wählen Sie aus dem Dropdown-Menü die Option **[Weitergeleitete Verbindung]** .
Erweitert	Wählen Sie die Option **[Externes Organisationsnetzwerk – Verbindung mit NAT-Routing]** .

5 Wählen Sie ein externes Netzwerk und einen Netzwerkpool aus und klicken Sie dann auf **[Weiter]** .

Wenn Sie das Kontrollkästchen **[Nur Netzwerke verwenden, auf die diese Organisation zugreifen kann]** deaktivieren, werden auch externe Netzwerke und Netzwerkpools angezeigt, die der Organisation aktuell nicht durch ihre Organisations-vDCs verfügbar gemacht wurden. Wenn Sie dieses Kontrollkästchen deaktivieren, können Sie ein beliebiges Netzwerk oder einen beliebigen Netzwerkpool auswählen und später ein Organisations-vDC erstellen, das auf das Netzwerk oder den Netzwerkpool zugreifen kann.

6 Verwenden Sie die Standardnetzwerkeinstellungen oder ändern Sie sie wie gewünscht und klicken Sie dann auf **[Weiter]** .

7 (Optional) Geben Sie die externe IP-Adresse zur Verwendung durch die NAT-Dienste ein, klicken Sie auf **[Hinzufügen]** und klicken Sie dann auf **[Weiter]** .

Diese Einstellung ist nur in der erweiterten Einrichtung verfügbar. Sie können mehrere externe IP-Adressen hinzufügen.

8 Geben Sie einen Namen und bei Bedarf eine Beschreibung ein und klicken Sie dann auf **[Weiter]** .

9 Überprüfen Sie die Einstellungen für das Organisationsnetzwerk.

Klicken Sie auf **[Fertigstellen]** , um die Einstellungen zu übernehmen und das Organisationsnetzwerk zu erstellen, oder klicken Sie auf **[Zurück]** , um die Einstellungen zu bearbeiten.

Weiter

Wenn Sie externe IP-Adressen hinzugefügt haben, können Sie deren Zuordnung festlegen. Siehe „Konfigurieren der Portweiterleitung für ein Organisationsnetzwerk“, auf Seite 64.

Erstellen eines internen Organisationsnetzwerks

Sie können ein internes Organisationsnetzwerk erstellen, auf das ausschließlich diese Organisation zugreifen kann. Das neue Netzwerk stellt für die Organisation ein internes Netzwerk bereit, zu dem mehrere vApps eine Verbindung herstellen können.

Voraussetzungen

Stellen Sie sicher, dass ein Netzwerkpool vorhanden ist.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationsnetzwerke]** .

2 Klicken Sie auf **[Netzwerk hinzufügen]** .

3 Wählen Sie eine Organisation aus und klicken Sie dann auf **[Weiter]** .

4 Wählen Sie den gewünschten Einrichtungstyp und den Netzwerktyp aus und klicken Sie dann auf **[Weiter]** .

Sie können ein internes Organisationsnetzwerk mithilfe einer der beiden folgenden Methoden erstellen.

Option	Netzwerktyp
Typisch	Aktivieren Sie das Kontrollkästchen für internes Netzwerk.
Erweitert	Wählen Sie die Option **[Internes Organisationsnetzwerk]** .

5 Wählen Sie einen Netzwerkpool aus und klicken Sie dann auf **[Weiter]** .

Wenn Sie das Kontrollkästchen **[Nur Netzwerke verwenden, auf die diese Organisation zugreifen kann]** deaktivieren, werden auch Netzwerkpools angezeigt, die der Organisation aktuell nicht durch ihre Organisations-vDCs verfügbar gemacht wurden. Wenn Sie dieses Kontrollkästchen deaktivieren, können Sie einen beliebigen Netzwerkpool auswählen und später ein Organisations-vDC erstellen, das auf ihn zugreifen kann.

6 Verwenden Sie die Standardnetzwerkeinstellungen oder ändern Sie sie wie gewünscht und klicken Sie dann auf **[Weiter]** .

7 Geben Sie einen Namen und bei Bedarf eine Beschreibung ein und klicken Sie dann auf **[Weiter]** .

8 Überprüfen Sie die Einstellungen für das Organisationsnetzwerk.

Klicken Sie auf **[Fertigstellen]** , um die Einstellungen zu übernehmen und das Organisationsnetzwerk zu erstellen, oder klicken Sie auf **[Zurück]** , um die Einstellungen zu bearbeiten.

Konfigurieren von Netzwerkdiensten

Sie können für bestimmte Organisationsnetzwerke Netzwerkdienste wie DHCP, Firewalls, NAT (Network Address Translation, Netzwerkadressenübersetzung) und VPN konfigurieren. Darüber hinaus können Organisationsadministratoren bestimmte Netzwerkdienste für ihre Organisationsnetzwerke konfigurieren.

Tabelle 5-5 enthält eine Liste der von vCloud Director für die verschiedenen Arten von Organisationsnetzwerken bereitgestellten Netzwerkdienste.

Tabelle 5-5. Verfügbare Netzwerkdienste nach Netzwerktypen

Netzwerktyp	DHCP	Firewall	NAT	VPN
Externes Organisationsnetzwerk – direkte Verbindung				
Externes Organisationsnetzwerk – Verbindung mit NAT-Routing	X	X	X	X
Internes Organisationsnetzwerk	X			

Konfigurieren von DHCP für ein Organisationsnetzwerk

Sie können bestimmte Organisationsnetzwerke so konfigurieren, dass für die virtuellen Maschinen in der Organisation DHCP-Dienste zur Verfügung stehen.

Wenn Sie für ein Organisationsnetzwerk DHCP aktivieren und über eine Netzwerkkarte in einer virtuellen Maschine in der Organisation eine Verbindung zu dem Netzwerk hergestellt werden soll, können Sie als IP-Modus für die Netzwerkkarte **[DHCP]** festlegen. vCloud Director weist dann dieser virtuellen Maschine beim Einschalten per DHCP eine IP-Adresse zu.

Sowohl Systemadministratoren als auch Organisationsadministratoren können DHCP konfigurieren.

Voraussetzungen

Ein externes Organisationsnetzwerk mit NAT-Routing oder ein internes Organisationsnetzwerk.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationsnetzwerke]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des Organisationsnetzwerks und wählen Sie den Befehl **[Dienste konfigurieren]** .

3 Klicken Sie auf die Registerkarte **[DHCP]** und wählen Sie die Option **[DHCP aktivieren]** .

4 Geben Sie einen IP-Adressbereich ein oder verwenden Sie den vorgegebenen Bereich.

   vCloud Director verwendet diese Adressen, um auf DHCP-Anforderungen zu antworten. Die IP-Adressbereiche für DHCP und für den statischen IP-Pool in dem Organisationsnetzwerk dürfen sich nicht überlagern.

5 Legen Sie die Standard-Lease-Dauer und die maximale Lease-Dauer fest, oder übernehmen Sie die entsprechenden Standardeinstellungen.

6 Klicken Sie auf **[OK]** .

vCloud Director aktualisiert die Netzwerkkonfiguration und stellt den DHCP-Dienst im Netzwerk bereit.

Aktivieren der Firewall für ein Organisationsnetzwerk

Sie können bestimmte Organisationsnetzwerke für die Bereitstellung von Firewalldiensten konfigurieren. Sie können die Firewall für ein Organisationsnetzwerk aktivieren, um die Einhaltung von Firewallregeln für eingehenden oder ausgehenden Datenverkehr oder für beides zu erzwingen.

Sie können den gesamten eingehenden oder den gesamten ausgehenden Datenverkehr oder beides verweigern. Sie können auch spezifische Firewallregeln hinzufügen, mit denen festgelegt wird, ob Datenverkehr, der den Regeln entspricht, die Firewall passieren darf oder nicht. Diese Regeln haben Vorrang vor den allgemeinen Regeln für das Durchlassen oder Verweigern des gesamten ein- oder ausgehenden Datenverkehrs. Weitere Informationen erhalten Sie unter „Hinzufügen einer Firewallregel für ein Organisationsnetzwerk“, auf Seite 61.

Systemadministratoren und Organisationsadministratoren können Firewalls aktivieren.

Voraussetzungen

Stellen Sie sicher, dass ein externes Organisationsnetzwerk mit NAT-Routing vorhanden ist.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationsnetzwerke]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des Organisationsnetzwerks und wählen Sie **[Dienste konfigurieren]** aus.

3 Klicken Sie auf die Registerkarte **[Firewall]** und wählen Sie die Option **[Firewall aktivieren]** .

4 Wählen Sie die Standardfirewallaktion aus.

5 (Optional) Aktivieren Sie das Kontrollkästchen **[Protokollieren]** , um mit der Standardfirewallaktion verbundene Ereignisse zu protokollieren.

6 Klicken Sie auf **[OK]** .

Hinzufügen einer Firewallregel für ein Organisationsnetzwerk

Sie können einem Organisationsnetzwerk Firewall-Regeln hinzufügen, die den Betrieb einer Firewall unterstützen. Sie können Regeln erstellen, die ein Passieren des den Regeln entsprechenden Netzwerkverkehrs durch die Firewall zulassen oder verweigern.

Sie müssen die Firewall für das Organisationsnetzwerk aktivieren, damit die Firewallregel erzwungen werden kann. Weitere Informationen erhalten Sie unter „Aktivieren der Firewall für ein Organisationsnetzwerk“, auf Seite 61.

Wenn Sie eine neue Firewallregel zu einem Organisationsnetzwerk hinzufügen, wird sie am Ende der Liste der Firewallregeln angezeigt. Informationen darüber, wie Sie die Reihenfolge festlegen, in der Firewallregeln erzwungen werden, erhalten Sie unter „Ändern der Reihenfolge von Firewallregeln für ein Organisationsnetzwerk“, auf Seite 62.

Systemadministratoren und Organisationsadministratoren können Firewallregeln hinzufügen.

Voraussetzungen

Stellen Sie sicher, dass ein externes Organisationsnetzwerk mit NAT-Routing vorhanden ist.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationsnetzwerke]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des Organisationsnetzwerks und wählen Sie **[Dienste konfigurieren]** aus.

3 Klicken Sie auf die Registerkarte **[Firewall]** und klicken Sie dann auf **[Hinzufügen]** .

4 Geben Sie einen Namen für die Regel ein.

5 Wählen Sie die Richtung des Netzwerkverkehrs aus.

6 Geben Sie die IP-Adresse der Quelle ein und wählen Sie den Quellport aus.

   Bei eingehendem Datenverkehr ist das externe Netzwerk die Quelle. Bei ausgehendem Datenverkehr ist das Organisationsnetzwerk die Quelle.

7 Geben Sie die IP-Adresse des Ziels ein und wählen Sie den Zielport aus.

   Bei eingehendem Datenverkehr ist das Organisationsnetzwerk das Ziel. Bei ausgehendem Datenverkehr ist das externe Netzwerk das Ziel.

8 Wählen Sie das Protokoll aus.

9 Wählen Sie die gewünschte Aktion aus.

   Eine Firewall-Regel kann Datenverkehr, welcher der Regel entspricht, zulassen oder verweigern.

10 Aktivieren Sie das Kontrollkästchen **[Aktiviert]** .

11 (Optional) Aktivieren Sie das Kontrollkästchen **[Netzwerkverkehr für Firewall-Regel protokollieren]** .

   Wenn Sie diese Option aktivieren, sendet vCloud Director für Verbindungen, die von dieser Regel betroffen sind, Protokollereignisse an den Syslog-Server. Jede Syslog-Nachricht enthält logische Netzwerk- und Organisations-UUIDs.

12 Klicken Sie auf **[OK]** und danach wieder auf **[OK]** .

Ändern der Reihenfolge von Firewallregeln für ein Organisationsnetzwerk

Firewallregeln werden in der Reihenfolge erzwungen, in der sie in der Firewallliste stehen. Sie können die Reihenfolge der Regeln in der Liste ändern.

Wenn Sie eine neue Firewallregel zu einem Organisationsnetzwerk hinzufügen, wird sie am Ende der Liste der Firewallregeln angezeigt. Wenn Sie die neue Regel vor einer vorhandenen Regel erzwingen möchten, müssen Sie die Reihenfolge der Regeln ändern.

Voraussetzungen

Ein Organisationsnetzwerk mit Routing mit mindestens zwei Firewallregeln.

Vorgehensweise

1 Klicken Sie auf **[Administration]** .

2 Wählen Sie **[Cloud-Ressourcen] > [Netzwerke]** .

3 Klicken Sie mit der rechten Maustaste auf den Namen des Organisationsnetzwerks und wählen Sie **[Dienste konfigurieren]** aus.

4 Klicken Sie auf die Registerkarte **[Firewall]** .

5 Verschieben Sie die Firewallregeln per Drag-und-Drop, um die Reihenfolge festzulegen, in der die Regeln angewendet werden.

6 Klicken Sie auf **[OK]** .

Aktivieren der IP-Maskierung für ein Organisationsnetzwerk

Sie können bestimmte Organisationsnetzwerke so konfigurieren, dass sie IP-Maskierungsdienste bereitstellen. Sie können die IP-Maskierung für ein Organisationsnetzwerk verwenden, um die interne IP-Adresse von virtuellen Maschinen vor dem externen Netzwerk zu verbergen.

Wenn Sie die IP-Maskierung aktivieren, übersetzt vCloud Director die private interne IP-Adresse einer virtuellen Maschine für ausgehenden Datenverkehr in eine öffentliche IP-Adresse.

Sowohl Systemadministratoren als auch Organisationsadministratoren können die IP-Maskierung aktivieren.

Voraussetzungen

Stellen Sie sicher, dass ein externes Organisationsnetzwerk mit NAT-Routing vorhanden ist.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationsnetzwerke]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des Organisationsnetzwerks und wählen Sie **[Dienste konfigurieren]** aus.

3 Klicken Sie auf die Registerkarte **[NAT-Zuordnung]** und wählen Sie die Option **[IP-Maskierung aktivieren]** .

4 Klicken Sie auf **[OK]** .

Hinzufügen von externen IP-Adressen zu einem Organisationsnetzwerk

Bevor Sie die NAT-Zuordnung für ein Organisationsnetzwerk konfigurieren können, müssen Sie zuerst eine oder mehrere externe IP-Adressen hinzufügen.

Die Berechtigung zum Hinzufügen von externen IP-Adressen zu einem Organisationsnetzwerk ist nur Systemadministratoren vorbehalten.

Voraussetzungen

Ein externes Organisationsnetzwerk mit NAT-Routing

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationsnetzwerke]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des Organisationsnetzwerks und wählen Sie **[Dienste konfigurieren]** aus.

3 Klicken Sie auf die Registerkarte **[NAT – Externe IPs]** .

4 Geben Sie eine IP-Adresse ein und klicken Sie dann auf **[Hinzufügen]** .

Die IP-Adresse muss an das externe Netzwerk weitergeleitet werden können und sie muss in allen internen Netzwerken eindeutig sein.

5 Klicken Sie auf **[OK]** .

Weiter

Konfigurieren Sie die NAT-Zuordnung unter Verwendung der externen IP-Adressen.

Konfigurieren der Portweiterleitung für ein Organisationsnetzwerk

Sie können bestimmte Organisationsnetzwerke für die Portweiterleitung konfigurieren. Die Portweiterleitung ermöglicht den Zugriff von externer Seite auf Dienste, die auf virtuellen Maschinen im Organisationsnetzwerk ausgeführt werden.

Wenn Sie die Portweiterleitung konfigurieren, ordnet vCloud Director einem auf dem Port einer virtuellen Maschine ausgeführten Dienst für eingehenden Datenverkehr eine externe IP-Adresse und einen Port zu.

Wenn Sie eine neue Portweiterleitungsregel zu einem Organisationsnetzwerk hinzufügen, wird diese am Ende der Liste der NAT-Zuordnungsregeln angezeigt. Informationen darüber, wie Sie die Reihenfolge festlegen, in der die NAT-Zuordnungsregeln erzwungen werden, erhalten Sie unter „Ändern der Reihenfolge von NAT-Zuordnungsregeln für ein Organisationsnetzwerk“, auf Seite 65.

Sowohl Systemadministratoren als auch Organisationsadministratoren können die Portweiterleitung konfigurieren.

Voraussetzungen

Stellen Sie sicher, dass ein externes Organisationsnetzwerk mit NAT-Routing und eine externe IP-Adresse vorhanden sind.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationsnetzwerke]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des Organisationsnetzwerks und wählen Sie **[Dienste konfigurieren]** aus.

3 Klicken Sie auf die Registerkarte **[NAT-Zuordnung]** und klicken Sie dann auf **[Hinzufügen]** .

4 Wählen Sie **[Portweiterleitung]** und konfigurieren Sie die Portweiterleitungsregel.

   a Wählen Sie eine externe IP-Adresse aus.

   b Wählen Sie einen externen Port aus.

   c Geben Sie die IP-Adresse der virtuellen Zielmaschine ein.

      - Wenn es sich um eine virtuelle Maschine mit Fencing handelt, geben Sie die externe IP-Adresse ein.
      - Andernfalls geben Sie die interne IP-Adresse der virtuellen Maschine ein.

   d Wählen Sie einen internen Port aus.

   e Wählen Sie ein Protokoll für den Typ des weiterzuleitenden Datenverkehrs aus.

   f Klicken Sie auf **[OK]** .

5 Klicken Sie auf **[OK]** .

Konfigurieren der IP-Übersetzung für ein Organisationsnetzwerk

Sie können bestimmte Organisationsnetzwerke für die Umsetzung von IP-Adressen ("IP-Übersetzung") konfigurieren.

Wenn Sie eine neue IP-Übersetzungsregel zu einem Organisationsnetzwerk hinzufügen, wird diese am Ende der Liste der NAT-Zuordnungsregeln angezeigt. Informationen darüber, wie Sie die Reihenfolge festlegen, in der die NAT-Zuordnungsregeln erzwungen werden, erhalten Sie unter „Ändern der Reihenfolge von NAT-Zuordnungsregeln für ein Organisationsnetzwerk“, auf Seite 65.

Wenn Sie eine IP-Übersetzungsregel für ein Netzwerk erstellen, fügt vCloud Director der mit der Portgruppe des Netzwerks verknüpften vShield Edge-Ressource eine DNAT- und eine SNAT-Regel hinzu. Die DNAT-Regel steuert die Umsetzung einer externen IP-Adresse in eine interne IP-Adresse für eingehenden Datenverkehr. Die SNAT-Regel steuert die Umsetzung einer internen IP-Adresse in eine externe IP-Adresse für ausgehenden Datenverkehr. Wenn das Netzwerk außerdem IP-Maskierung verwendet, hat die SNAT-Regel Vorrang.

Sowohl Systemadministratoren als auch Organisationsadministratoren können die IP-Übersetzung konfigurieren.

Voraussetzungen

Ein externes Organisationsnetzwerk mit NAT-Routing und eine externe IP-Adresse

Vorgehensweise

1. Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationsnetzwerke]** .
2. Klicken Sie mit der rechten Maustaste auf den Namen des Organisationsnetzwerks und wählen Sie **[Dienste konfigurieren]** aus.
3. Klicken Sie auf die Registerkarte **[NAT-Zuordnung]** und klicken Sie dann auf **[Hinzufügen]** .
4. Wählen Sie **[IP-Übersetzung]** und konfigurieren Sie die Regel.
   a. Wählen Sie eine externe IP-Adresse aus.
   b. Geben Sie die IP-Adresse der virtuellen Zielmaschine ein.
      - Wenn es sich um eine virtuelle Maschine mit Fencing handelt, geben Sie die externe IP-Adresse ein.
      - Andernfalls geben Sie die IP-Adresse der virtuellen Maschine ein.
   c. Klicken Sie auf **[OK]** .
5. Klicken Sie auf **[OK]** .

Ändern der Reihenfolge von NAT-Zuordnungsregeln für ein Organisationsnetzwerk

NAT-Zuordnungsregeln werden in der Reihenfolge erzwungen, in der sie in der Liste der NAT-Zuordnungen stehen. Ein Organisationsadministrator kann die Reihenfolge der Regeln in der Liste ändern.

Wenn Sie eine neue NAT-Zuordnungsregel (beispielsweise IP-Übersetzung oder Portweiterleitung) zu einem Organisationsnetzwerk hinzufügen, wird sie am Ende der Liste der NAT-Zuordnungsregeln angezeigt. Um die neue Regel vor einer vorhandenen Regel zu erzwingen, ändern Sie die Reihenfolge der Regeln.

Voraussetzungen

Stellen Sie sicher, dass ein Organisationsnetzwerk mit Routing und mindestens zwei NAT-Zuordnungsregeln vorhanden ist.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationsnetzwerke]** .
2. Klicken Sie mit der rechten Maustaste auf den Namen des Organisationsnetzwerks und wählen Sie **[Dienste konfigurieren]** aus.
3. Klicken Sie auf die Registerkarte **[NAT-Zuordnung]** .
4. Klicken Sie und ziehen Sie die Regeln per Drag-und-Drop, um die Reihenfolge festzulegen, in der sie angewendet werden.

5 Klicken Sie auf **[OK]** .

Aktivieren von Site-to-Site-VPN für ein Organisationsnetzwerk

Sie können Site-to-Site-VPN-Konfigurationen für ein Organisationsnetzwerk aktivieren und anschließend einen sicheren VPN-Tunnel zu einem anderen Netzwerk erstellen.

vCloud Director unterstützt Site-to-Site-VPN-Konfigurationen zwischen Organisationsnetzwerken innerhalb derselben Organisation, Organisationsnetzwerken in unterschiedlichen Organisationen (einschließlich Organisationsnetzwerken in verschiedenen Instanzen von vCloud Director) und Remotenetzwerken.

Sowohl Systemadministratoren als auch Organisationsadministratoren können Site-to-Site-VPN aktivieren.

Voraussetzungen

- Ein externes Organisationsnetzwerk mit NAT-Routing
- vShield Manager 5.0.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationsnetzwerke]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des Organisationsnetzwerks und wählen Sie **[Dienste konfigurieren]** aus.

3 Klicken Sie auf die Registerkarte **[Site-to-Site-VPN]** und wählen Sie dann **[Site-to-Site-VPN aktivieren]** .

4 (Optional) Geben Sie eine öffentliche IP-Adresse ein.

Wenn das externe Netzwerk, zu dem das Organisationsnetzwerk weitergeleitet wird, sich hinter einem NAT-Gerät befindet, müssen Sie eine vom Internet her öffentlich zugängliche IP-Adresse bereitstellen.

5 Klicken Sie auf **[OK]** .

Weiter

Erstellen eines VPN-Tunnels zu einem anderen Netzwerk.

Erstellen eines VPN-Tunnels innerhalb einer Organisation

Sie können zwischen zwei Organisationsnetzwerken derselben Organisation einen VPN-Tunnel erstellen.

Sowohl Systemadministratoren als auch Organisationsadministratoren können VPN-Tunnel erstellen.

Wenn zwischen den Tunnelendpunkten eine Firewall vorhanden ist, müssen Sie sie so konfigurieren, dass sie die folgenden IP-Protokolle und UDP-Ports zulässt:

- IP-Protokoll-ID 50 (ESP)
- IP-Protokoll-ID 51 (AH)
- UDP-Port 500 (IKE)
- UDP-Port 4500

Voraussetzungen

- Mindestens zwei externe Organisationsnetzwerke mit NAT-Routing und nicht überlappenden IP-Subnetzen sowie aktivierter Unterstützung für Site-to-Site-VPN-Konfigurationen.
- vShield Manager 5.0.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationsnetzwerke]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des Organisationsnetzwerks und wählen Sie **[Dienste konfigurieren]** aus.

3 Klicken Sie auf die Registerkarte **[Site-to-Site-VPN]** und klicken Sie dann auf **[Hinzufügen]** .

4 Geben Sie einen Namen und bei Bedarf eine Beschreibung ein.

5 Wählen Sie die Option **[ein Netzwerk in dieser Organisation]** aus dem Dropdown-Menü und danach ein Peer-Netzwerk aus.

6 Überprüfen Sie die Tunneleinstellungen und klicken Sie auf **[OK]** .

vCloud Director konfiguriert beide Peer-Netzwerk-Endpunkte.

Erstellen eines VPN-Tunnels zwischen Organisationen

Sie können zwischen zwei Organisationsnetzwerken in unterschiedlichen Organisationen einen VPN-Tunnel erstellen. Die Organisationen können zu einer und derselben vCloud Director-Installation oder unterschiedlichen Installationen gehören.

Sowohl Systemadministratoren als auch Organisationsadministratoren können VPN-Tunnel erstellen.

Wenn zwischen den Tunnelendpunkten eine Firewall vorhanden ist, müssen Sie sie so konfigurieren, dass sie die folgenden IP-Protokolle und UDP-Ports zulässt:

- IP Protocol ID 50 (ESP)
- IP Protocol ID 51 (AH)
- UDP-Port 500 (IKE)
- UDP-Port 4500

Voraussetzungen

- Jeweils ein externes Organisationsnetzwerk mit NAT-Weiterleitung in jeder beteiligten Organisation. Die Organisationsnetzwerke müssen über nicht überlappende IP-Subnetze verfügen und Site-to-Site-VPN-Konfigurationen unterstützen.
- vShield Manager 5.0.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationsnetzwerke]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des Organisationsnetzwerks und wählen Sie **[Dienste konfigurieren]** aus.

3 Klicken Sie auf die Registerkarte **[Site-to-Site-VPN]** und klicken Sie dann auf **[Hinzufügen]** .

4 Geben Sie einen Namen und bei Bedarf eine Beschreibung ein.

5 Wählen Sie die Option **[einem Netzwerk in einer anderen Organisation]** aus dem Dropdown-Menü.

6 Klicken Sie auf **[Mit einer anderen Organisation verbinden]** , geben Sie die Anmeldeinformationen für die Peer-Organisation ein und klicken Sie auf **[Fortfahren]** .

Option	Beschreibung
vCloud-URL	Die Basis-URL der vCloud-Instanz, welche die Peer-Organisation enthält. Beispiel: **`https://www.beispiel.com`**. Die URL darf weder **`/cloud`** noch **`/cloud/org/`*`orgname`*** enthalten.
Organisation	Der als eindeutiger Bezeichner in der Organisations-URL verwendete Organisationsname. Beispiel: Wenn die Organisations-URL **`https://www.beispiel.com/cloud/org/meineOrg`** lautet, müssen Sie **`meineOrg`** eingeben.
Benutzername	Der Benutzername eines Organisations- oder Systemadministrators, der Zugriff auf die Organisation hat.
Kennwort	Das mit dem Benutzernamen verknüpfte Kennwort.

7 Wählen Sie ein Peer-Netzwerk aus.

8 Überprüfen Sie die Tunneleinstellungen und klicken Sie auf **[Verbinden]** .

vCloud Director konfiguriert beide Peer-Netzwerk-Endpunkte.

Erstellen eines VPN-Tunnels zu einem Remotenetzwerk

Sie können zwischen einem Organisationsnetzwerk und einem Remotenetzwerk einen VPN-Tunnel erstellen.

Sowohl Systemadministratoren als auch Organisationsadministratoren können VPN-Tunnel erstellen.

Wenn zwischen den Tunnelendpunkten eine Firewall vorhanden ist, müssen Sie sie so konfigurieren, dass sie die folgenden IP-Protokolle und UDP-Ports zulässt:

- IP-Protokoll-ID 50 (ESP)
- IP-Protokoll-ID 51 (AH)
- UDP-Port 500 (IKE)
- UDP-Port 4500

Voraussetzungen

- Ein externes Organisationsnetzwerk mit NAT-Routing oder ein Remotenetzwerk mit Routing, das IPSec verwendet.
- vShield Manager 5.0.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationsnetzwerke]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des Organisationsnetzwerks und wählen Sie **[Dienste konfigurieren]** aus.

3 Klicken Sie auf die Registerkarte **[Site-to-Site-VPN]** und klicken Sie dann auf **[Hinzufügen]** .

4 Geben Sie einen Namen und bei Bedarf eine Beschreibung ein.

5 Wählen Sie die Option **[ein Remotenetzwerk]** aus dem Dropdown-Menü.

6 Geben Sie die Peer-Einstellungen ein.

7 Überprüfen Sie die Tunneleinstellungen und klicken Sie auf **[OK]** .

vCloud Director konfiguriert den Endpunkt des Organisations-Peer-Netzwerks.

Weiter

Konfigurieren Sie den Endpunkt des Remote-Peer-Netzwerks manuell.

Aktivieren des statischen Routings für ein Organisationsnetzwerk

Sie können bestimmte Organisationsnetzwerke so konfigurieren, dass sie statische Routingdienste bieten. Nachdem Sie das statische Routing auf einem Organisationsnetzwerk aktiviert haben, können Sie statische Routen hinzufügen, um Datenverkehr zwischen verschiedenen vApp-Netzwerken mit Routing zum Organisationsnetzwerk zuzulassen.

Voraussetzungen

Stellen Sie sicher, dass ein Organisationsnetzwerk mit Routing vorhanden ist.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationsnetzwerke]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des Organisationsnetzwerks und wählen Sie **[Dienste konfigurieren]** aus.

3 Wählen Sie auf der Registerkarte **[Statisches Routing]** die Option **[Statisches Routing aktivieren]** und klicken Sie auf **[OK]** .

Weiter

Erstellen Sie statische Routen. Weitere Informationen erhalten Sie unter „Hinzufügen von statischem Routing zwischen vApp-Netzwerken mit Routing zum selben Organisationsnetzwerk“, auf Seite 69 und „Hinzufügen von statischem Routing zwischen vApp-Netzwerken mit Routing zu verschiedenen Organisationsnetzwerken“, auf Seite 71.

Hinzufügen von statischem Routing zwischen vApp-Netzwerken mit Routing zum selben Organisationsnetzwerk

Sie können statisches Routing zwischen zwei vApp-Netzwerken mit Routing zum selben Organisationsnetzwerk hinzufügen. Statisches Routing ermöglicht Datenverkehr zwischen den Netzwerken.

Zwischen überlappenden Netzwerken oder vApps mit Fencing können Sie kein statisches Routing hinzufügen. Nachdem Sie ein statisches Routing zu einem Organisationsnetzwerk hinzugefügt haben, konfigurieren Sie die Netzwerkfirewallregeln so, dass sie Datenverkehr auf dem statischen Routing zulassen.

Statisches Routing funktioniert nur, wenn die in den Routen enthaltenen vApps ausgeführt werden. Wenn Sie das übergeordnete Netzwerk einer vApp ändern, eine vApp löschen oder ein vApp-Netzwerk löschen und die vApp statische Routen enthält, können diese Routen nicht mehr funktionieren. Sie müssen sie dann manuell entfernen.

Voraussetzungen

Stellen Sie sicher, dass die Netzwerke wie folgt konfiguriert sind:

- vShield 5.0.
- Ein Organisationsnetzwerk mit Routing
- Das statische Routing ist auf dem Organisationsnetzwerk aktiviert.
- Zwei vApp-Netzwerke mit Routing zum Organisationsnetzwerk.
- Die vApp-Netzwerke befinden sich in vApps, die mindestens ein Mal gestartet wurden.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationsnetzwerke]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des Organisationsnetzwerks und wählen Sie **[Dienste konfigurieren]** aus.

3 Klicken Sie auf der Registerkarte **[Statisches Routing]** auf **[Hinzufügen]** .

4 Geben Sie einen Namen, die Netzwerkadresse und die IP des nächsten Hops ein.

Die Netzwerkadresse ist für das erste vApp-Netzwerk bestimmt, zu dem Sie statisches Routing hinzufügen möchten. Die IP des nächsten Hops ist die externe IP-Adresse des Routers des vApp-Netzwerks.

5 Wählen Sie **[Innerhalb dieses Netzwerks]** und klicken Sie auf **[OK]** .

6 Klicken Sie auf **[OK]** .

7 Wiederholen Sie die Schritte Schritt 3 bis Schritt 6, um eine Route zu dem zweiten vApp-Netzwerk hinzuzufügen.

Beispiel: Statisches Routing – Beispiel

vApp-Netzwerk 1 und vApp-Netzwerk 2 werden beide zum freigegebenen Organisationsnetzwerk weitergeleitet. Sie können statisches Routing auf dem Organisationsnetzwerk erstellen, um Datenverkehr zwischen den vApp-Netzwerken zuzulassen. Sie können die statischen Routen mithilfe von Informationen über die vApp-Netzwerke erstellen.

Tabelle 5-6. Netzwerkinformationen

Netzwerkname	Netzwerkspezifikation	Externe IP-Adresse des Routers
vApp-Netzwerk 1	192.168.1.0/24	192.168.0.100
vApp-Netzwerk 2	192.168.2.0/24	192.168.0.101
Freigegebenes Organisationsnetzwerk	192.168.0.0/24	n.v.

Erstellen Sie auf dem freigegebenen Organisationsnetzwerk eine statische Route zu vApp-Netzwerk 1 und eine weitere statische Route zu vApp-Netzwerk 2.

Tabelle 5-7. Statisches Routing – Einstellungen

Statisches Routing zum Netzwerk	Name der Route	Netzwerk	IP-Adresse des nächsten Hops	Route
vApp-Netzwerk 1	zuvapp1	192.168.1.0/24	192.168.0.100	Innerhalb dieses Netzwerks
vApp-Netzwerk 2	zuvapp2	192.168.2.0/24	192.168.0.101	Innerhalb dieses Netzwerks

Weiter

Erstellen Sie Firewallregeln, um Datenverkehr auf den statischen Routen zuzulassen. Weitere Informationen erhalten Sie unter „Hinzufügen einer Firewallregel für ein Organisationsnetzwerk“, auf Seite 61.

Hinzufügen von statischem Routing zwischen vApp-Netzwerken mit Routing zu verschiedenen Organisationsnetzwerken

Ein Organisationsadministrator kann statisches Routing zwischen zwei vApp-Netzwerken mit Routing zu verschiedenen Organisationsnetzwerken hinzufügen. Statisches Routing ermöglicht Datenverkehr zwischen den Netzwerken.

Zwischen überlappenden Netzwerken oder vApps mit Fencing können Sie kein statisches Routing hinzufügen. Nachdem Sie ein statisches Routing zu einem Organisationsnetzwerk hinzugefügt haben, konfigurieren Sie die Netzwerkfirewallregeln so, dass sie Datenverkehr auf dem statischen Routing zulassen. Aktivieren Sie für vApps mit statischen Routen das Kontrollkästchen **[Verwenden Sie immer zugeordnete IP-Adressen, bis diese vApp oder zugehörige Netzwerke gelöscht sind]** .

Statisches Routing funktioniert nur, wenn die in den Routen enthaltenen vApps ausgeführt werden. Wenn Sie das übergeordnete Netzwerk einer vApp ändern, eine vApp löschen oder ein vApp-Netzwerk löschen und die vApp statische Routen enthält, können diese Routen nicht funktionieren. Sie müssen sie dann manuell entfernen.

Voraussetzungen

Stellen Sie sicher, dass vCloud Director wie folgt konfiguriert ist:

- vShield 5.0.
- Zwei Organisationsnetzwerke mit Routing zum selben externen Netzwerk.
- Das statische Routing ist auf beiden Organisationsnetzwerken aktiviert.
- Ein vApp-Netzwerk mit Routing zu jedem Organisationsnetzwerk.
- Die vApp-Netzwerke befinden sich in vApps, die mindestens ein Mal gestartet wurden.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationsnetzwerke]** .
2. Klicken Sie mit der rechten Maustaste auf den Namen des Organisationsnetzwerks und wählen Sie **[Dienste konfigurieren]** aus.
3. Klicken Sie auf der Registerkarte **[Statisches Routing]** auf **[Hinzufügen]** .
4. Geben Sie einen Namen, die Netzwerkadresse und die IP-Adresse des nächsten Hops ein.

   Die Netzwerkadresse ist für das vApp-Netzwerk bestimmt, zu dem Sie statisches Routing hinzufügen möchten. Die IP-Adresse des nächsten Hops ist die externe IP-Adresse des Routers für das Organisationsnetzwerk, zu dem dieses vApp-Netzwerk weitergeleitet wird.
5. Wählen Sie **[Zum externen Netzwerk]** und klicken Sie auf **[OK]** .
6. Klicken Sie auf **[Hinzufügen]** .
7. Geben Sie einen Namen, die Netzwerkadresse und die IP-Adresse des nächsten Hops ein.

   Die Netzwerkadresse ist für das vApp-Netzwerk bestimmt, das zu diesem Organisationsnetzwerk weitergeleitet wird. Die IP-Adresse des nächsten Hops ist die externe IP-Adresse des Routers für dieses vApp-Netzwerk.
8. Wählen Sie **[Innerhalb dieses Netzwerks]** und klicken Sie auf **[OK]** .
9. Wiederholen Sie die Schritte Schritt 3 bis Schritt 8, um statische Routen zu dem zweiten Organisationsnetzwerk hinzuzufügen.

Beispiel: Statisches Routing – Beispiel

vApp-Netzwerk 1 wird zu Organisationsnetzwerk 1 weitergeleitet. vApp-Netzwerk 2 wird zu Organisationsnetzwerk 2 weitergeleitet. Sie können statisches Routing auf den Organisationsnetzwerken erstellen, um Datenverkehr zwischen den vApp-Netzwerken zuzulassen. Sie können statisches Routing mithilfe von Informationen über die vApp-Netzwerke und Organisationsnetzwerke erstellen.

Tabelle 5-8. Netzwerkinformationen

Netzwerkname	Netzwerkspezifikation	Externe IP-Adresse des Routers
vApp-Netzwerk 1	192.168.1.0/24	192.168.0.100
vApp-Netzwerk 2	192.168.11.0/24	192.168.10.100
Organisationsnetzwerk 1	192.168.0.0/24	10.112.205.101
Organisationsnetzwerk 2	192.168.10.0/24	10.112.205.100

Erstellen Sie auf Organisationsnetzwerk 1 eine statische Route zu vApp-Netzwerk 2 und eine weitere statische Route zu vApp-Netzwerk 1. Erstellen Sie auf Organisationsnetzwerk 2 eine statische Route zu vApp-Netzwerk 1 und eine weitere statische Route zu vApp-Netzwerk 2.

Tabelle 5-9. Statisches Routing – Einstellungen für Organisationsnetzwerk 1

Statisches Routing zum Netzwerk	Name der Route	Netzwerk	IP-Adresse des nächsten Hops	Route
vApp-Netzwerk 2	zuvapp2	192.168.11.0/24	10.112.205.100	Zum externen Netzwerk
vApp-Netzwerk 1	zuvapp1	192.168.1.0/24	192.168.0.100	Innerhalb dieses Netzwerks

Tabelle 5-10. Statisches Routing – Einstellungen für Organisationsnetzwerk 2

Statisches Routing zum Netzwerk	Name der Route	Netzwerk	IP-Adresse des nächsten Hops	Route
vApp-Netzwerk 1	zuvapp1	192.168.1.0/24	10.112.205.101	Zum externen Netzwerk
vApp-Netzwerk 2	zuvapp2	192.168.11.0/24	192.168.10.100	Innerhalb dieses Netzwerks

Weiter

Erstellen Sie Firewallregeln, um Datenverkehr auf den statischen Routen zuzulassen. Weitere Informationen erhalten Sie unter „Hinzufügen einer Firewallregel für ein Organisationsnetzwerk“, auf Seite 61.

Zurücksetzen eines Organisationsnetzwerks

Wenn die Netzwerkdienste, z. B. DHCP- oder Firewalleinstellungen, für ein Organisationsnetzwerk nicht wie erwartet funktionieren, können Sie das Netzwerk zurücksetzen.

Bevor Sie ein Provider-vDC löschen, setzen Sie die Organisationsnetzwerke zurück, die von ihm abhängig sind.

Während ein Organisationsnetzwerk zurückgesetzt wird, sind keine Netzwerkdienste verfügbar.

Voraussetzungen

Stellen Sie sicher, dass ein externes Organisationsnetzwerk mit NAT-Routing oder ein internes Organisationsnetzwerk vorhanden sind.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationsnetzwerke]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des Organisationsnetzwerks und wählen Sie den Befehl **[Netzwerk zurücksetzen]** .

3 Klicken Sie auf **[Ja]** .

Anzeigen von vApps und vApp-Vorlagen, die ein Organisationsnetzwerk verwenden

Sie können eine Liste aller vApps und vApp-Vorlagen anzeigen, die virtuelle Maschinen mit einem Netzwerkadapter enthalten, der mit einem Organisationsnetzwerk verbunden ist. Ein Organisationsnetzwerk mit verbundenen vApps oder vApp-Vorlagen kann nicht gelöscht werden.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationsnetzwerke]** .

2 Wählen Sie ein Organisationsnetzwerk aus, klicken Sie mit der rechten Maustaste, und wählen Sie **[Verbundene vApps]** .

3 Klicken Sie auf **[OK]** .

Löschen eines Organisationsnetzwerks

Sie können ein Organisationsnetzwerk löschen, um es aus der Organisation zu entfernen.

Voraussetzungen

Stellen Sie sicher, dass keine virtuellen Maschinen mit dem Organisationsnetzwerk verbunden sind. Weitere Informationen erhalten Sie unter „Anzeigen von vApps und vApp-Vorlagen, die ein Organisationsnetzwerk verwenden“, auf Seite 73.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationsnetzwerke]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des Organisationsnetzwerks und wählen Sie den Befehl **[Löschen]** .

Anzeigen der IP-Nutzung für ein Organisationsnetzwerk

Sie können eine Liste der IP-Adressen anzeigen, die derzeit in einem Netzwerk-IP-Pool einer Organisation verwendet werden.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationsnetzwerke]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des Organisationsnetzwerks und wählen Sie den Befehl **[IP-Zuweisungen]** .

Hinzufügen von IP-Adressen zum IP-Pool eines Organisationsnetzwerks

Wenn in einem Organisationsnetzwerk nicht mehr genügend IP-Adressen verfügbar sind, können Sie dem zugehörigen IP-Pool weitere IP-Adressen hinzufügen.

Voraussetzungen

Ein externes Organisationsnetzwerk mit NAT-Routing oder ein internes Organisationsnetzwerk.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationsnetzwerke]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des Organisationsnetzwerks und wählen Sie den Befehl **[Eigenschaften]** .

3 Geben Sie auf der Registerkarte **[Netzwerkspezifikation]** eine IP-Adresse oder einen Bereich von IP-Adressen in das Textfeld ein, und klicken Sie auf **[Hinzufügen]** .

4 Klicken Sie auf **[OK]** .

Bearbeiten des Netzwerknamens und der Beschreibung eines Organisationsnetzwerks

Wenn Ihre vCloud Director-Installation anwächst, besteht möglicherweise Bedarf, einer bestehenden Organisation einen aussagekräftigeren Namen oder eine Beschreibung zuzuweisen.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationsnetzwerke]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des Organisationsnetzwerks und wählen Sie den Befehl **[Eigenschaften]** .

3 Geben Sie auf der Registerkarte **[Name und Beschreibung]** einen neuen Namen und bei Bedarf eine optionale Beschreibung ein und klicken Sie auf **[OK]** .

Bearbeiten der DNS-Einstellungen eines Organisationsnetzwerks

Bei bestimmten Arten von Organisationsnetzwerken können Sie die DNS-Einstellungen ändern.

Voraussetzungen

Ein externes Organisationsnetzwerk mit NAT-Routing oder ein internes Organisationsnetzwerk.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationsnetzwerke]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des Organisationsnetzwerks und wählen Sie den Befehl **[Eigenschaften]** .

3 Geben Sie auf der Registerkarte **[Netzwerkspezifikation]** die neuen DNS-Daten ein und klicken Sie auf **[OK]** .

Anzeigen von Syslog-Servereinstellungen für ein Organisationsnetzwerk

Sie können die Syslog-Servereinstellungen für ein Organisationsnetzwerk mit Routing anzeigen.

vCloud Director unterstützt die Protokollierung von mit Firewallregeln verbundenen Ereignissen auf einem von einem Systemadministrator festgelegten Syslog-Server.

Wenn ein Organisationsnetzwerk nicht über Syslog-Servereinstellungen verfügt, Sie dies jedoch ändern möchten, oder wenn die Einstellungen nicht Ihren Erwartungen entsprechen, synchronisieren Sie das Netzwerk mit den aktuellsten Syslog-Servereinstellungen. Weitere Informationen erhalten Sie unter „Anwenden von Syslog-Servereinstellungen auf ein Organisationsnetzwerk“, auf Seite 75.

Voraussetzungen

- Stellen Sie sicher, dass ein externes Organisationsnetzwerk mit NAT-Routing vorhanden ist.
- Stellen Sie sicher, dass Sie über Organisationsadministrator-Rechte verfügen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationsnetzwerke]** .
2. Wählen Sie ein Organisationsnetzwerk, klicken Sie mit der rechten Maustaste, und wählen Sie **[Eigenschaften]** aus.
3. Klicken Sie auf die Registerkarte **[Syslog-Servereinstellungen]** .

Anwenden von Syslog-Servereinstellungen auf ein Organisationsnetzwerk

Sie können Syslog-Servereinstellungen auf ein Organisationsnetzwerk mit Routing anwenden, um die Protokollierung von Firewallregeln zu aktivieren.

Wenden Sie Syslog-Servereinstellungen auf alle Organisationsnetzwerke an, die vor der erstmaligen Erstellung dieser Einstellungen erstellt wurden. Außerdem müssen die Syslog-Servereinstellungen auf ein Organisationsnetzwerk angewendet werden, sobald die Einstellungen geändert wurden.

Wenn Sie nicht genau wissen, ob die Syslog-Einstellungen eines Organisationsnetzwerks auf dem neuesten Stand sind, können Sie die Syslog-Einstellungen des Organisationsnetzwerks anzeigen. Weitere Informationen erhalten Sie unter „Anzeigen von Syslog-Servereinstellungen für ein Organisationsnetzwerk“, auf Seite 74.

Voraussetzungen

Stellen Sie sicher, dass ein externes Organisationsnetzwerk mit NAT-Routing vorhanden ist.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationsnetzwerke]** .
2. Wählen Sie ein Organisationsnetzwerk, klicken Sie mit der rechten Maustaste und wählen Sie **[Syslog-Servereinstellungen synchronisieren]** .
3. Klicken Sie auf **[Ja]** .

Verwalten von Netzwerkpools

Wenn Sie einen Netzwerkpool erstellt haben, können Sie seinen Namen und seine Beschreibung bearbeiten und den Pool löschen. Je nach Typ des Netzwerkpools können Sie dem Pool darüber hinaus Portgruppen, cloudisolierte Netzwerke und VLAN-IDs hinzufügen.

Bearbeiten des Namens und der Beschreibung eines Netzwerkpools

Wenn Ihre vCloud Director-Installation anwächst, besteht möglicherweise Bedarf, einem bestehenden Netzwerkpool einen aussagekräftigeren Namen oder eine Beschreibung zuzuweisen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Netzwerkpools]** .
2. Klicken Sie mit der rechten Maustaste auf den Netzwerkpoolnamen und wählen Sie den Befehl **[Eigenschaften]** .

3 Geben Sie auf der Registerkarte **[Allgemein]** einen neuen Namen oder eine neue Beschreibung ein und klicken Sie auf **[OK]** .

Hinzufügen einer Portgruppe zu einem Netzwerkpool

Sie können Portgruppen zu einem portgruppenbasierten Netzwerkpool hinzufügen.

Voraussetzungen

- Prüfen Sie, ob ein von einer Portgruppe gestützter Netzwerkpool vorhanden ist
- Prüfen Sie, ob in vSphere eine verfügbare Portgruppe vorhanden ist

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Netzwerkpools]** .

2 Klicken Sie mit der rechten Maustaste auf den Netzwerkpoolnamen und wählen Sie den Befehl **[Eigenschaften]** .

3 Wählen Sie auf der Registerkarte **[Netzwerkpooleinstellungen]** eine Portgruppe aus, klicken Sie auf **[Hinzufügen]** und dann auf **[OK]** .

Hinzufügen von cloudisolierten Netzwerken zu einem Netzwerkpool

Sie können Netzwerkpools, die durch VCD-Netzwerkisolation gestützt werden, cloudisolierte Netzwerke hinzufügen.

Voraussetzungen

Ein Netzwerkpool, der durch VCD-Netzwerkisolation gestützt wird

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Netzwerkpools]** .

2 Klicken Sie mit der rechten Maustaste auf den Netzwerkpoolnamen und wählen Sie den Befehl **[Eigenschaften]** .

3 Geben Sie auf der Registerkarte **[Netzwerkpooleinstellungen]** die Anzahl der VCD-isolierten Netzwerke ein und klicken Sie dann auf **[OK]** .

Hinzufügen von VLAN-IDs zu einem Netzwerkpool

Sie können VLAN-IDs zu einem VLAN-gestützten Netzwerkpool hinzufügen.

Voraussetzungen

Prüfen Sie, ob Folgendes im System enthalten ist:

- Ein Netzwerkpool, der durch ein VLAN gestützt wird
- Verfügbare VLAN-IDs in vSphere

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Netzwerkpools]** .

2 Klicken Sie mit der rechten Maustaste auf den Netzwerkpoolnamen und wählen Sie den Befehl **[Eigenschaften]** .

3 Geben Sie auf der Registerkarte **[Netzwerkpooleinstellungen]** einen VLAN-ID-Bereich ein und klicken Sie auf **[Hinzufügen]** .

4 Wählen Sie einen vSphere Distributed Switch aus und klicken Sie dann auf **[OK]** .

Löschen eines Netzwerkpools

Löschen Sie einen Netzwerkpool, um ihn aus vCloud Director zu entfernen.

Voraussetzungen

Prüfen Sie, ob die folgenden Bedingungen erfüllt sind:

- Dem Netzwerkpool ist kein Organisations-vDC zugeordnet.
- Der Netzwerkpool wird nicht von vApps verwendet.
- Der Netzwerkpool wird nicht von Organisationsnetzwerken mit NAT-Routing oder internen Organisationsnetzwerken verwendet.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Netzwerkpools]** .

2 Klicken Sie mit der rechten Maustaste auf den Netzwerkpoolnamen und wählen Sie den Befehl **[Löschen]** .

3 Klicken Sie auf **[Ja]** .

Verwalten von Cloud-Zellen

Sie verwalten Cloud-Zellen hauptsächlich über den vCloud Director-Serverhost, auf dem sich die Zellen befinden. Das Löschen einer Cloud-Zelle kann jedoch auch über die vCloud Director-Webkonsole erfolgen.

Tabelle 5-11 sind die grundlegenden Befehle zur Steuerung einer Cloud-Zelle aufgelistet.

Tabelle 5-11. Befehle für Cloud-Zellen

Befehl	Beschreibung
`service vmware-vcd start`	Startet die Zelle
`service vmware-vcd restart`	Startet die Zelle erneut
`service vmware-vcd stop`	Beendet die Zelle

Wenn Sie eine Zelle beenden, kann es erwünscht sein, eine Wartungsmeldung für Benutzer anzuzeigen, die versuchen, mithilfe eines Browsers oder der vCloud-API auf diese Zelle zuzugreifen. Weitere Informationen hierzu erhalten Sie unter „Aktivieren der Wartungsmeldung für Cloud-Zellen“, auf Seite 78.

Hinzufügen von Cloud-Zellen

Um einer vCloud Director-Installation Cloud-Zellen hinzuzufügen, installieren Sie die vCloud Director-Software auf zusätzlichen Cloud Director-Serverhosts innerhalb desselben vCloud Director-Clusters.

Weitere Informationen erhalten Sie im *Installations- und Konfigurationshandbuch zu VMware vCloud Director*.

Löschen einer Cloud-Zelle

Wenn Sie zwecks Neuinstallation der Software oder aus einem anderen Grund eine Cloud-Zelle aus einer vCloud Director-Installation entfernen möchten, können Sie die Zelle löschen.

Sie können eine Zelle auch löschen, wenn sie nicht mehr erreichbar ist.

Voraussetzungen

Sie müssen die Zelle mit dem Befehl `service vmware-vcd stop` anhalten.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Cloud-Zellen]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen der Zelle und wählen Sie den Befehl **[Löschen]** .

vCloud Director entfernt die Informationen zur Zelle aus der Datenbank.

Aktivieren der Wartungsmeldung für Cloud-Zellen

Wenn Sie eine Zelle beenden und die Benutzer über die aktuell stattfindenden Wartungsarbeiten informieren möchten, können Sie die Wartungsmeldung aktivieren.

Wenn die Wartungsmeldung aktiviert ist, wird Benutzern, die versuchen, sich über den Browser bei der Zelle anzumelden, eine Meldung angezeigt, die ihnen mitteilt, dass die Zelle zu Wartungszwecken außer Betrieb ist. Benutzer, die versuchen, unter Verwendung der vCloud-API auf die Zelle zuzugreifen, erhalten eine ähnliche Meldung.

Vorgehensweise

1 Beenden Sie die Zelle mit dem Befehl `service vmware-vcd stop`.

2 Führen Sie den Befehl `/opt/vmware/cloud-director/bin/vmware-vcd-cell maintenance` aus.

Benutzer können jetzt nicht mehr mithilfe eines Browsers oder der vCloud-API auf die Zelle zugreifen.

Deaktivieren der Wartungsmeldung für Cloud-Zellen

Wenn Sie die Wartungsarbeiten für eine Zelle beendet haben und die Zelle neu gestartet werden kann, können Sie die Wartungsmeldung deaktivieren.

Vorgehensweise

1 Führen Sie den Befehl `/opt/vmware/cloud-director/bin/vmware-vcd-cell stop` aus.

2 Starten Sie die Zelle mit dem Befehl `service vmware-vcd start`.

Benutzer können jetzt mithilfe eines Browsers oder der vCloud-API auf die Zelle zugreifen.

Verwalten von vSphere-Ressourcen 6

Nach dem Hinzufügen von vSphere-Ressourcen zum vCloud Director-System können Sie in vCloud Director bestimmte Verwaltungsfunktionen durchführen. Alternativ können Sie diese Ressourcen auch mit dem vSphere Client verwalten.

vSphere-Ressourcen sind u. a. vCenter Server, Ressourcenpools, ESX/ESXi-Hosts und Datenspeicher sowie Netzwerkswitches und Ports.

Dieses Kapitel behandelt die folgenden Themen:

- „Verwalten von vSphere vCenter Server“, auf Seite 79
- „Verwalten von vSphere ESX/ESXi-Hosts“, auf Seite 81
- „Verwalten von vSphere-Datenspeichern“, auf Seite 83
- „Verwalten freigelegter Objekte“, auf Seite 84

Verwalten von vSphere vCenter Server

Nach dem Anfügen von vCenter Server an vCloud Director können Sie seine Einstellungen bearbeiten, erneut eine Verbindung zum vCenter Server herstellen sowie ihn aktivieren und deaktivieren.

Registrieren von vCloud Director bei einem vCenter Server

Sie können vCloud Director bei dem von ihm verwendeten vCenter Server registrieren.

Nach seiner Registrierung wird vCloud Director als Erweiterung auf der Solution-Manager-Registerkarte des vSphere Client angezeigt. Außerdem legt der vSphere Client die **[///Managed By]** -Eigenschaft für von vCloud Director verwaltete virtuelle Maschinen fest und schützt damit diese virtuellen Maschinen vor Modifikationen mithilfe des vSphere Client.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[vCenter]** .
2. Klicken Sie mit der rechten Maustaste auf den Namen des vCenter Server und wählen Sie den Befehl **[Aktualisieren]** .
3. Klicken Sie auf **[Ja]** .

Bearbeiten der vCenter Server-Einstellungen

Wenn die Verbindungseinstellungen für ein vCenter Server geändert werden oder Sie die Anzeige des Namens bzw. der Beschreibung in vCloud Director ändern möchten, können Sie diese Einstellungen bearbeiten.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[vCenter]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen von vCenter Server und wählen Sie den Befehl **[Eigenschaften]** .

3 Geben Sie auf der Registerkarte **[Allgemein]** die neuen Einstellungen ein und klicken Sie auf **[OK]** .

Erneutes Verbinden mit einem vCenter Server

Wenn vCloud Director die Verbindung zu einem vCenter Server verliert oder Sie die Verbindungseinstellungen ändern, können Sie versuchen, die Verbindung wiederherzustellen.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[vCenter]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen von vCenter Server und wählen Sie den Befehl **[vCenter erneut verbinden]** .

3 Lesen Sie die Informationen in der Meldung und klicken Sie auf **[Ja]** , um den Vorgang zu bestätigen.

Aktivieren oder Deaktivieren von vCenter Server

Sie können einen vCenter Server deaktivieren, um Wartungen durchzuführen.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[vCenter]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen von vCenter Server und wählen Sie den Befehl **[Deaktivieren]** bzw. **[Aktivieren]** .

3 Klicken Sie auf **[Ja]** .

Entfernen von vCenter Server

Sie können einen vCenter Server entfernen, damit seine Ressourcen in vCloud Director nicht mehr verwendet werden.

Voraussetzungen

Um einen vCenter Server entfernen zu können, müssen Sie ihn deaktivieren und alle Provider-vDCs löschen, die seine Ressourcenpools verwenden.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[vCenter]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen von vCenter Server und wählen Sie den Befehl **[Anfügung aufheben]** .

3 Klicken Sie auf **[Ja]** .

Vorbereiten und Aktualisieren eines an vCloud Director angefügten vCenter Server

Bevor Sie einen an vCloud Director angefügten vCenter Server aktualisieren, müssen Sie den Server vorbereiten, indem Sie ihn in vCloud Director deaktivieren.

Machen Sie sich mit der Dokumentation zu *vSphere-Upgrade* vertraut.

Vorgehensweise

1 Klicken Sie in der vCloud Director-Webkonsole auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[vCenter]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen der vCenter Server-Instanz und wählen Sie den Befehl **[Deaktivieren]** .

3 Klicken Sie auf **[Ja]** .

4 Aktualisieren Sie vCenter Server.

5 Klicken Sie in der vCloud Director-Webkonsole mit der rechten Maustaste auf den Namen der vCenter Server-Instanz und wählen Sie den Befehl **[Aktivieren]** .

6 Klicken Sie auf **[Ja]** .

Weiter

Registrieren Sie vCloud Director mit dem aktualisierten Server. Weitere Informationen erhalten Sie unter „Registrieren von vCloud Director bei einem vCenter Server“, auf Seite 79.

Bearbeiten der vShield Manager-Einstellungen

Wenn die Verbindungseinstellungen für den vShield Manager für ein vCenter Server geändert werden oder Sie einen anderen vShield Manager verwenden möchten, können Sie diese Einstellungen bearbeiten.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[vCenter]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen von vCenter Server und wählen Sie den Befehl **[Eigenschaften]** .

3 Geben Sie auf der Registerkarte **[vShield Manager]** die neuen Einstellungen ein und klicken Sie auf **[OK]** .

Verwalten von vSphere ESX/ESXi-Hosts

Sie können Hosts für die Verwendung mit vCloud Director vorbereiten, aktivieren und deaktivieren, aktualisieren und reparieren.

Aktivieren oder Deaktivieren eines ESX/ESXi-Hosts

Sie können einen Host deaktivieren, um zu verhindern, dass auf dem Host vApps gestartet werden. Virtuelle Maschinen, die zu diesem Zeitpunkt bereits auf dem Host ausgeführt werden, sind nicht betroffen.

Wenn Sie an einem Host Wartungen durchführen müssen, migrieren Sie alle vApps zu einem anderen Host und deaktivieren Sie dann den ersten Host.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Hosts]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des Hosts und wählen Sie den Befehl **[Host aktivieren]** bzw. **[Host deaktivieren]** .

vCloud Director aktiviert bzw. deaktiviert den Host für alle Provider-vDCs, die dessen Ressourcen verwenden.

Verschieben von virtuellen Maschinen zwischen ESX/ESXi-Hosts

Sie können beliebige virtuelle Maschinen von einem ESX/ESXi-Host auf beliebige andere Hosts in demselben Cluster verschieben. Dies ist nützlich, um ohne Auswirkungen auf die laufenden Maschinen die Vorbereitung eines Hosts rückgängig zu machen oder Wartungsarbeiten auf einem Host durchzuführen.

Voraussetzungen

Deaktivieren Sie den Host.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Hosts]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des Hosts und wählen Sie den Befehl **[Alle VMs erneut bereitstellen]** .

3 Klicken Sie auf **[Ja]** .

vCloud Director versetzt den Host in den Wartungsmodus und verschiebt seine virtuelle Maschinen auf andere Hosts in demselben Cluster.

Vorbereiten eines ESX/ESXi-Hosts oder Rückgängigmachen der Vorbereitung

Wenn Sie einem vSphere-Cluster, der von vCloud Director verwendet wird, einen ESX/ESXi-Host hinzufügen, müssen Sie den Host vorbereiten, bevor Provider-vDCs seine Ressourcen nutzen können. Sie können die Vorbereitung eines Hosts auch rückgängig machen, um ihn aus der vCloud Director-Umgebung zu entfernen.

Informationen zum Verschieben von virtuellen Maschinen zwischen Hosts erhalten Sie unter „Verschieben von virtuellen Maschinen zwischen ESX/ESXi-Hosts“, auf Seite 82.

Hosts, die sich im gesperrten Modus befinden, können nicht vorbereitet werden. Nach dem Vorbereiten eines Hosts kann er in den gesperrten Modus versetzt werden.

Voraussetzungen

Deaktivieren Sie den Host, und stellen Sie sicher, dass auf dem Host keine virtuellen Maschinen laufen.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Hosts]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des Hosts und wählen Sie den Befehl **[Host vorbereiten]** bzw. **[Vorbereitung für Host rückgängig]** .

3 Wenn Sie einen Host vorbereiten möchten, geben Sie einen Benutzernamen und das zugehörige Kennwort ein und klicken Sie auf **[OK]** .

vCloud Director bereitet den Host für alle Provider-vDCs vor, die dessen Ressourcen verwenden, bzw. macht die Vorbereitung rückgängig.

Aktualisieren eines ESX/ESXi-Host-Agenten

vCloud Director installiert die Agent-Software auf allen ESX/ESXi-Hosts in der Installation. Wenn Sie Ihre ESX/ESXi-Hosts aktualisieren, müssen Sie gleichzeitig auch Ihre ESX/ESXi-Host-Agents aktualisieren.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Hosts]** .

2 Klicken Sie mit der rechten Maustaste auf den Benutzernamen und wählen Sie den Befehl **[Host-Agent-Upgrade]** .

Reparieren eines ESX/ESXi-Hosts

Wenn auf einem ESX/ESXi-Host der vCloud Director-Agent nicht mehr antwortet, versuchen Sie, den Host zu reparieren.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Hosts]** .

2 Klicken Sie mit der rechten Maustaste auf den Benutzernamen und wählen Sie den Befehl **[Host reparieren]** .

Verwalten von vSphere-Datenspeichern

Sie können vSphere-Datenspeicher im vCloud Director-System aktivieren oder deaktivieren, Warnungen zu niedrigem verbleibenden Speicherplatz auf Festplatten für Datenspeicher konfigurieren und Datenspeicher aus dem vCloud Director-System entfernen.

Die einzige Möglichkeit, vCloud Director-Systemen einen Datenspeicher hinzuzufügen, besteht darin, ihn einem Provider-vDC hinzuzufügen. Siehe „Hinzufügen von Speicherkapazität zu einem Provider-vDC“, auf Seite 46.

Aktivieren oder Deaktivieren eines Datenspeichers

Sie können einen zu einem Provider-vDC hinzugefügten Datenspeicher aktivieren oder deaktivieren. Sie müssen einen Datenspeicher deaktivieren, bevor Sie ihn aus vCloud Director entfernen können.

Wenn Sie einen Datenspeicher deaktivieren, können diesem Datenspeicher zugeordnete vApps nicht mehr gestartet werden. Außerdem können auf dem Datenspeicher keine vApps mehr erstellt werden.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Datenspeicher]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen des Datenspeichers und wählen Sie den Befehl **[Aktivieren]** bzw. **[Deaktivieren]** .

vCloud Director aktiviert bzw. deaktiviert den Datenspeicher für alle Provider-vDCs, die dessen Ressourcen verwenden.

Entfernen eines Datenspeichers

Sie können einen Datenspeicher aus vCloud Director entfernen, um zu verhindern, dass Provider-vDCs seine Speicherressourcen verwenden.

Voraussetzungen

Stellen Sie sicher, dass der Datenspeicher deaktiviert ist und aus allen Provider-vDCs entfernt wurde, die ihn verwenden.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Datenspeicher]** .
2. Klicken Sie mit der rechten Maustaste auf den Namen des Datenspeichers und wählen Sie den Befehl **[Entfernen]** .
3. Klicken Sie auf **[Ja]** .

vCloud Director entfernt den Datenspeicher.

Konfigurieren der Warnmeldungen über zu niedrige verbleibende Festplattenkapazität für Datenspeicher

Sie können Warnmeldungen über zu niedrige verbleibende Festplattenkapazität auf einem Datenspeicher so konfigurieren, dass vCloud Director mit dem Erreichen eines bestimmten Schwellenwertes zur verfügbaren Kapazität eine entsprechende Warnmeldung per E-Mail versendet. Diese E-Mail-Nachricht dient dazu, Sie von der Situation des geringen verbleibenden Speicherplatzes in Kenntnis zu setzen, bevor dies problematisch werden könnte.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Datenspeicher]** .
2. Klicken Sie mit der rechten Maustaste auf den Namen des Datenspeichers und wählen Sie den Befehl **[Eigenschaften]** .
3. Wählen Sie auf der Registerkarte **[Allgemein]** die Festplattenkapazität-Schwellenwerte für den Datenspeicher aus.

   Sie können zwei Schwellenwerte festlegen, einen gelben und einen roten. Wenn vCloud Director eine Warnmeldung per E-Mail versendet, wird auf dieser Nachricht vermerkt, welcher der beiden Schwellenwerte unterschritten wurde.
4. Klicken Sie auf **[OK]** .

vCloud Director versendet eine Warnmeldung per E-Mail, wenn ein Datenspeicher einen Schwellenwert unterschreitet.

Verwalten freigelegter Objekte

Wenn Sie in vCloud Director ein Objekt löschen, das auch in vSphere existiert, versucht vCloud Director, das Objekt auch aus vSphere zu löschen. In bestimmten Situationen ist vCloud Director möglicherweise jedoch nicht in der Lage, das Objekt in vSphere zu löschen, das dann als freigelegtes Objekt bezeichnet wird.

Sie können eine Liste der freigelegten Objekte anzeigen und erneut versuchen, sie zu löschen. Sie können auch den vSphere Client verwenden, um freigelegte Objekte in vSphere zu löschen.

Löschen eines isolierten Objekts

Sie können isolierte Objekte löschen, um auf diese Weise Objekte aus vSphere zu entfernen, die Sie bereits zuvor aus vCloud Director gelöscht haben.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Isolierte Objekte]** .

2 Klicken Sie mit der rechten Maustaste auf ein isoliertes Objekt und wählen Sie den Befehl **[Löschen]** .

3 Klicken Sie auf **[Ja]** .

vCloud Director versucht, das isolierte Objekt aus vSphere zu löschen.

4 Aktualisieren Sie die Seitenanzeige.

Wenn der Löschvorgang erfolgreich abgeschlossen wurde, entfernt vCloud Director das Objekt aus der Liste der isolierten Objekte.

Weiter

Wenn der Löschvorgang fehlschlägt, können Sie das Löschen dieser Objekte erzwingen. Siehe „Erzwungenes Löschen eines isolierten Objekts“, auf Seite 85.

Erzwungenes Löschen eines isolierten Objekts

Wenn vCloud Director ein isoliertes Objekt nicht löschen kann, können Sie das Löschen erzwingen, um es aus der Liste der isolierten Objekte zu entfernen. Das isolierte Objekt ist jedoch in vSphere weiterhin vorhanden.

Versuchen Sie, ein isoliertes Objekt zunächst einfach zu löschen, bevor Sie die Löschung erzwingen. Siehe „Löschen eines isolierten Objekts“, auf Seite 85.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Isolierte Objekte]** .

2 Klicken Sie mit der rechten Maustaste auf das isolierte Objekt und wählen Sie den Befehl **[Löschung erzwingen]** .

3 Klicken Sie auf **[Ja]** .

vCloud Director entfernt das Objekt aus der Liste der isolierten Objekte.

Verwalten von Organisationen 7

Wenn Sie eine Organisation erstellt haben, können Sie ihre Eigenschaften bearbeiten, sie aktivieren bzw. deaktivieren und löschen.

Dieses Kapitel behandelt die folgenden Themen:

- „Aktivieren oder Deaktivieren einer Organisation“, auf Seite 87
- „Löschen einer Organisation“, auf Seite 88
- „Bearbeiten des Organisationsnamens“, auf Seite 88
- „Bearbeiten des vollständigen Namens und der Beschreibung einer Organisation“, auf Seite 88
- „Bearbeiten der LDAP-Optionen für die Organisation“, auf Seite 89
- „Bearbeiten der Richtlinien zur Veröffentlichung von Katalogen für die Organisation“, auf Seite 90
- „Bearbeiten der E-Mail-Einstellungen für eine Organisation“, auf Seite 90
- „Bearbeiten von Lease-, Kontingent- und Grenzwerteinstellungen auf Organisationsebene“, auf Seite 91
- „Hinzufügen eines Katalogs zu einer Organisation“, auf Seite 92
- „Verwalten von Organisationsressourcen“, auf Seite 92
- „Verwalten der Benutzer und Gruppen von Organisationen“, auf Seite 92
- „Verwalten von Organisations-vApps und virtuellen Maschinen“, auf Seite 93

Aktivieren oder Deaktivieren einer Organisation

Wenn Sie eine Organisation deaktivieren, können sich keine Benutzer mehr bei der Organisation anmelden und die Sitzungen aktuell angemeldeter Benutzer werden beendet. Zu diesem Zeitpunkt innerhalb der Organisation ausgeführte vApps werden weiterhin ausgeführt.

Systemadministratoren können auch deaktivierten Organisationen Ressourcen zuweisen, Netzwerke hinzufügen usw.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationen]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen der Organisation und wählen Sie den Befehl **[Aktivieren]** bzw. **[Deaktivieren]** .

Löschen einer Organisation

Löschen Sie eine Organisation, um sie endgültig aus vCloud Director zu entfernen.

Voraussetzungen

Sie können eine Organisation erst dann löschen, wenn Sie sie deaktiviert und für alle Objekte, die von Benutzern der Organisation besitzt werden, den Besitzer gelöscht oder geändert haben.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisation]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen der Organisation und wählen Sie den Befehl **[Löschen]** .

3 Klicken Sie auf **[Ja]** .

Bearbeiten des Organisationsnamens

Wenn Ihre vCloud Director-Installation anwächst, besteht möglicherweise Bedarf, einer bestehenden Organisation einen aussagekräftigeren Namen zuzuweisen.

Voraussetzungen

Sie müssen die Organisation deaktivieren, damit Sie sie umbenennen können.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationen]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen der Organisation und wählen Sie den Befehl **[Eigenschaften]** .

3 Geben Sie auf der Registerkarte **[Allgemein]** einen neuen Namen für die Organisation ein und klicken Sie auf **[OK]** .

Die interne URL für die Organisation wird geändert und enthält nun den neuen Namen.

Bearbeiten des vollständigen Namens und der Beschreibung einer Organisation

Wenn Ihre vCloud Director-Installation anwächst, besteht möglicherweise Bedarf, einer bestehenden Organisation einen aussagekräftigeren vollständigen Namen oder eine Beschreibung zuzuweisen.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationen]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen der Organisation und wählen Sie den Befehl **[Eigenschaften]** .

3 Geben Sie auf der Registerkarte **[Allgemein]** einen neuen vollständigen Namen oder eine neue Beschreibung ein und klicken Sie auf **[OK]** .

Bearbeiten der LDAP-Optionen für die Organisation

Sie können einen LDAP-Dienst als Verzeichnis für Benutzer und Gruppen nutzen, die in eine Organisation importiert werden sollen. Wenn Sie keinen LDAP-Dienst angeben, müssen Sie die Benutzerkonten für die Benutzer in der Organisation einzeln erstellen. Die LDAP-Optionen können ausschließlich von einem Systemadministrator festgelegt werden. Organisationsadministratoren verfügen nicht über die erforderlichen Berechtigungen, diese Optionen zu bearbeiten.

Weitere Informationen zur Eingabe der LDAP-Einstellungen erhalten Sie unter „Konfigurieren der System-LDAP-Einstellungen“, auf Seite 108.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationen]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen der Organisation und wählen Sie den Befehl **[Eigenschaften]** .

3 Klicken Sie auf die Registerkarte **[LDAP-Optionen]** .

4 Wählen Sie die neue Quelle für Benutzer der Organisation aus.

Option	Beschreibung
LDAP nicht verwenden	Der Administrator der Organisation erstellt für alle Benutzer der Organisation ein lokales Benutzerkonto. Wenn Sie diese Option wählen, können Sie keine Gruppen erstellen.
LDAP-Dienst des VCD-Systems	Verwendet den LDAP-Dienst in dem vCloud Director-System als Quelle für Benutzer und Gruppen der Organisation.
LDAP-Dienst anpassen	Verbindet die Organisation mit ihrem eigenen, privaten LDAP-Dienst.

5 Geben Sie weitere Daten an, die für die ausgewählte Option erforderlich sind.

Option	Aktion
LDAP nicht verwenden	Klicken Sie auf **[OK]** .
LDAP-Dienst des VCD-Systems	(Optional) Geben Sie den distinktiven Namen der zu verwendenden Organisationseinheit (OU) ein, um die Menge der in die Organisation zu importierenden Benutzer einzuschränken, und klicken Sie dann auf **[OK]** . Wenn Sie keinen Wert eingeben, können alle Benutzer in dem System-LDAP-Dienst in die Organisation importiert werden. **Hinweis** Die Festlegung einer Organisationseinheit schränkt nicht die importierbaren LDAP-Gruppen ein. Sie können beliebige LDAP-Gruppen aus dem Root-Verzeichnis des System-LDAP-Verzeichnisses importieren. Allerdings können sich nur Benutzer, die sich in der Organisationseinheit und in der importierten Gruppe befinden, bei der Organisation anmelden.
LDAP-Dienst anpassen	Klicken Sie auf die Registerkarte **[Benutzerdefiniertes LDAP]** , geben Sie die benutzerdefinierten LDAP-Einstellungen für die Organisation ein und klicken Sie auf **[OK]** .

Systemadministratoren und Organisationsadministratoren, die aktuell angemeldet sind, können Benutzer und Gruppen erst dann unter Verwenden der geänderten LDAP-Optionen importieren, wenn der Cache für ihre aktuelle Sitzung abläuft oder sie sich ab- und wieder anmelden.

Bearbeiten der Richtlinien zur Veröffentlichung von Katalogen für die Organisation

Über Kataloge wird den Benutzern von Organisationen eine Bibliothek von vApp-Vorlagen und Medien bereitgestellt, die die Benutzer zum Erstellen von vApps nutzen können. Im Allgemeinen stehen Kataloge nur den Benutzern in einer einzigen Organisation zur Verfügung; Systemadministratoren können jedoch Organisationsadministratoren erlauben, Kataloge für alle Organisationen in der vCloud Director-Installation zu veröffentlichen.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationen]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen der Organisation und wählen Sie den Befehl **[Eigenschaften]** .

3 Klicken Sie auf die Registerkarte **[Katalogveröffentlichung]** .

4 Wählen Sie eine Option zur Katalogveröffentlichung aus und klicken Sie auf **[OK]** .

Option	Beschreibung
Kataloge können nicht veröffentlicht werden	Organisationsadministratoren können für Benutzer außerhalb ihrer Organisation keine Kataloge veröffentlichen.
Veröffentlichung von Katalogen bei allen Organisationen zulassen	Organisationsadministratoren können für Benutzer in allen Organisationen Kataloge veröffentlichen.

Bei Benutzern, die zum Zeitpunkt der Bearbeitung bei der Organisation angemeldet sind, werden Änderungen der Richtlinie zur Katalogveröffentlichung erst dann übernommen, wenn der Cache für die aktuelle Sitzung des Benutzers abläuft oder sich der Benutzer ab- und wieder anmeldet.

Bearbeiten der E-Mail-Einstellungen für eine Organisation

vCloud Director benötigt einen SMTP-Server, um E-Mails zur Benachrichtigung von Benutzern und zu Systemwarnungen zu versenden. Sie können die Einstellungen, die Sie beim Erstellen der Organisation festgelegt haben, ändern.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationen]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen der Organisation und wählen Sie den Befehl **[Eigenschaften]** .

3 Klicken Sie auf die Registerkarte **[E-Mail-Einstellungen]** .

4 Wählen Sie eine Option zu dem SMTP-Server aus.

Option	Beschreibung
Standard-SMTP-Server des Systems verwenden	Die Organisation verwendet den Standard-SMTP-Server des Systems.
SMTP-Server der Organisation festlegen	Die Organisation verwendet einen eigenen SMTP-Server. Wenn Sie diese Option wählen, geben Sie den DNS-Hostnamen oder die IP-Adresse des SMTP-Servers sowie die Portnummer ein. (Optional) Aktivieren Sie das Kontrollkästchen **[Authentifizierung erforderlich]** und geben Sie einen Benutzernamen und das zugehörige Kennwort ein.

5 Wählen Sie eine Option zu den Benachrichtigungseinstellungen aus.

Option	Beschreibung
Standard-Benachrichtigungseinstellungen des Systems verwenden	Die Organisation verwendet die Benachrichtigungseinstellungen des Systems.
Benachrichtigungseinstellungen der Organisation festlegen	Die Organisation verwendet eigene Benachrichtigungseinstellungen. Wenn Sie diese Option wählen, geben Sie eine E-Mail-Adresse ein, die als Absender für E-Mails der Organisation angezeigt wird, geben Sie desgleichen einen Text als Betreff ein und wählen Sie die Empfänger aus.

6 (Optional) Geben Sie eine Ziel-E-Mail-Adresse ein und klicken Sie auf **[E-Mail-Einstellungen testen]** , um zu überprüfen, ob die konfigurierten SMTP-Servereinstellungen wie erwartet funktionieren.

7 Klicken Sie auf **[OK]** .

Bearbeiten von Lease-, Kontingent- und Grenzwerteinstellungen auf Organisationsebene

Leases, Kontingente und Grenzwerte beschränken die Möglichkeit von Benutzern in der Organisation zur Nutzung von Speicher- und Prozessorressourcen. Bearbeiten Sie diese Einstellungen, um zu verhindern, dass einzelne Benutzer eine Ressource der Organisation erschöpfend oder ausschließlich nutzen.

Weitere Informationen zu Leases erhalten Sie unter „Grundlagen zu Leases“, auf Seite 23.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationen]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen der Organisation und wählen Sie den Befehl **[Eigenschaften]** .

3 Klicken Sie auf die Registerkarte **[Richtlinien]** .

4 Wählen Sie die gewünschten Lease-Optionen für vApps und vApp-Vorlagen aus.

Leases ermöglichen eine grundlegende Steuerung der Speicher- und Rechenressourcen, indem festgelegt wird, wie lange vApps maximal ausgeführt und wie lange vApps und vApp-Vorlagen gespeichert werden dürfen. Darüber hinaus können Sie festlegen, was mit den vApps bzw. vApp-Vorlagen geschieht, wenn der Speicher-Lease abläuft.

5 Wählen Sie die Kontingente für laufende und gespeicherte virtuelle Maschinen aus.

Kontingente legen fest, wie viele virtuelle Maschinen die einzelnen Benutzer in der Organisation in deren virtuellen Datencentern speichern und einschalten dürfen. Die festgelegten Kontingente werden für alle der Organisation neu hinzugefügten Benutzer als Standardwerte übernommen.

6 Wählen Sie die Grenzwerte für ressourcenintensive Operationen aus.

Bestimmte vCloud Director-Operationen, beispielsweise das Kopieren und Verschieben, verbrauchen mehr Ressourcen als andere. Mit diesen Grenzwerten können Sie verhindern, dass ressourcenintensive Operationen Auswirkungen auf alle anderen Benutzer in einer Organisation haben. Darüber hinaus bieten diese Grenzwerte einen Schutz gegen DoS-Angriffe.

7 Wählen Sie die Anzahl gleichzeitiger Verbindungen für die einzelnen virtuellen Maschinen aus und klicken Sie auf **[OK]** .

Hinzufügen eines Katalogs zu einer Organisation

Sie können für die hochgeladenen und importierten vApp-Vorlagen und -Mediendateien einen Katalog zu einer Organisation hinzufügen. Organisationen können über mehrere Kataloge verfügen, für die der Zugriff individuell geregelt werden kann.

Voraussetzungen

Prüfen Sie, ob eine Organisation vorhanden ist, in der ein Katalog erstellt werden kann.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Startseite]** und klicken Sie dann auf **[Weiteren Katalog zu einer Organisation hinzufügen]** .

2 Wählen Sie einen Organisationsnamen aus und klicken Sie dann auf **[Weiter]** .

3 Geben Sie einen Katalognamen und bei Bedarf eine Beschreibung ein und klicken Sie dann auf **[Weiter]** .

4 Wählen Sie die Veröffentlichungsoption aus und klicken Sie auf **[Weiter]** .

Option	Beschreibung
Diesen Katalog nicht bei anderen Organisationen veröffentlichen	Die Objekte, die dem Katalog hinzugefügt werden, sind nur innerhalb der Organisation verfügbar.
Bei allen Organisationen veröffentlichen	Die Objekte, die dem Katalog hinzugefügt werden, sind für alle Organisationen in der vCloud Director-Installation verfügbar. Die Administratoren der einzelnen Organisationen können wählen, welche Katalogobjekte sie für ihre Benutzer bereitstellen.

5 Überprüfen Sie die Katalogeinstellungen und klicken Sie auf **[Fertigstellen]** .

Verwalten von Organisationsressourcen

vCloud Director-Organisationen erhalten ihre Ressourcen für ein oder mehrere Organisations-vDCs. Wenn Sie für eine Organisation weitere Ressourcen benötigen, können Sie ein neues Organisations-vDC hinzufügen oder ein bestehendes Organisations-vDC bearbeiten. Sie können einer Organisation Ressourcen entziehen, indem Sie ein Organisations-vDC entfernen oder bearbeiten.

Weitere Informationen zum Hinzufügen von Organisations-vDCs erhalten Sie unter „Erstellen eines Organisations-vDC“, auf Seite 48.

Weitere Informationen zum Entfernen eines Organisations-vDC erhalten Sie unter „Löschen eines Organisations-vDCs“, auf Seite 53.

Weitere Informationen zum Bearbeiten der für ein bestehendes Organisations-vDC verfügbaren Ressourcen erhalten Sie unter „Bearbeiten der Einstellungen von Zuweisungsmodellen für Organisations-vDCs“, auf Seite 54 und „Bearbeiten der Speichereinstellungen von Organisations-vDCs“, auf Seite 54.

Verwalten der Benutzer und Gruppen von Organisationen

Wenn Sie eine Organisation erstellen, können Sie ihr einen oder mehrere lokale Benutzer hinzufügen. Nachdem eine Organisation erstellt ist, können Sie (oder ein Organisationsadministrator) ihr lokale Benutzer, LDAP-Benutzer und LDAP-Gruppen hinzufügen.

Weitere Informationen zum Hinzufügen von Benutzern und Gruppen zu einer Organisation erhalten Sie im *VMware vCloud Director-Benutzerhandbuch*.

Verwalten von Organisations-vApps und virtuellen Maschinen

Einige Aufgaben in Zusammenhang mit der Verwaltung von Organisations-vApps und virtuellen Maschinen können ausschließlich von einem Systemadministrator durchgeführt werden. Systemadministratoren können beispielsweise virtuelle vSphere-Maschinen zu einer vorhandenen vApp hinzufügen, eine vApp auf der Grundlage einer virtuellen vSphere-Maschine erstellen und eine vApp in den Wartungsmodus versetzen.

Weitere Informationen zum Arbeiten mit vApps in einer Organisation erhalten Sie im *VMware vCloud Director-Benutzerhandbuch*.

Hinzufügen einer virtuellen vSphere-Maschine zu einer vApp

Systemadministratoren können eine virtuelle vSphere-Maschine in eine vorhandene vCloud Director-vApp importieren.

Voraussetzungen

Sie müssen als Systemadministrator bei vCloud Director angemeldet sein, und die Organisation, die die vApp enthält, muss über ein verfügbares Organisations-vDC verfügen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationen]** .
2. Klicken Sie mit der rechten Maustaste auf den Namen der Organisation und wählen Sie den Befehl **[Öffnen]** .
3. Klicken Sie auf die Registerkarte **[Meine Cloud]** und klicken Sie dann im linken Bereich auf **[vApps]** .
4. Klicken Sie mit der rechten Maustaste auf den Namen der vApp und wählen Sie den Befehl **[Öffnen]** .
5. Klicken Sie auf der Registerkarte **[Virtuelle Maschinen]** auf die Schaltfläche **[Aktionen]** und wählen Sie **[Von vSphere importieren]** .
6. Wählen Sie einen vCenter Server und eine virtuelle Maschine aus.
7. Geben Sie einen Namen und bei Bedarf eine Beschreibung für die virtuelle Maschine ein.
8. Wählen Sie aus, ob Sie die virtuelle Maschine, die als Quelle verwendet werden soll, kopieren oder verschieben möchten.
9. Klicken Sie auf **[OK]** .

Erstellen einer vApp auf der Grundlage einer virtuellen vSphere-Maschine

Systemadministratoren können eine virtuelle vSphere-Maschine als vCloud Director-vApp in eine Organisation importieren.

Voraussetzungen

Stellen Sie sicher, dass Sie als Systemadministrator bei vCloud Director angemeldet sind und die Organisation ein verfügbares Organisations-vDC besitzt.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationen]** .
2. Klicken Sie mit der rechten Maustaste auf den Namen der Organisation und wählen Sie den Befehl **[Öffnen]** .
3. Klicken Sie auf die Registerkarte **[Meine Cloud]** und klicken Sie dann im linken Bereich auf **[vApps]** .

4 Klicken Sie auf **[Von vSphere importieren]** .

5 Wählen Sie einen vCenter Server und eine virtuelle Maschine aus.

6 Geben Sie einen Namen und bei Bedarf eine Beschreibung für die vApp ein und wählen Sie das Ziel-Organisations-vDC aus.

7 Wählen Sie aus, ob Sie die virtuelle Maschine, die als Quelle verwendet werden soll, kopieren oder verschieben möchten.

8 Klicken Sie auf **[OK]** .

Versetzen einer vApp in den Wartungsmodus

Ein Systemadministrator kann eine vApp in den Wartungsmodus versetzen, damit der Status der vApp nicht von Benutzern, die keine Administratoren sind, geändert werden kann. Dies ist beispielsweise dann nützlich, wenn Sie eine vApp mit einer Sicherungslösung eines Fremdherstellers sichern möchten.

Wenn sich eine vApp im Wartungsmodus befindet, können Benutzer, die keine Systemadministratoren sind, keine Aktionen durchführen, die den Status der vApp oder ihrer virtuellen Maschine ändern. Sie können Informationen über die vApp und ihre virtuellen Maschinen anzeigen und auf die Konsolen der virtuellen Maschine zugreifen.

Das Versetzen einer vApp in den Wartungsmodus hat keine Auswirkungen auf laufende Aufgaben, in die die vApp involviert ist.

Voraussetzungen

Sie müssen als Systemadministrator bei vCloud Director angemeldet sein.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationen]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen der Organisation und wählen Sie den Befehl **[Öffnen]** .

3 Klicken Sie auf die Registerkarte **[Meine Cloud]** und klicken Sie dann im linken Bereich auf **[vApps]** .

4 Klicken Sie mit der rechten Maustaste auf den Namen der vApp und wählen Sie **[In den Wartungsmodus wechseln]** aus.

5 Klicken Sie auf **[Ja]** .

Der Status der vApp wird in **[Im Wartungsmodus]** geändert. Die vApp bleibt so lange im Wartungsmodus, bis Sie **[Wartungsmodus beenden]** auswählen.

Erzwungenes Beenden einer ausgeführten vApp

Systemadministratoren können das Beenden einer ausgeführten vApp erzwingen, wenn ein Benutzer in der Organisation dazu nicht in der Lage ist.

In bestimmten Fällen können Benutzer eine ausgeführte vApp möglicherweise nicht mehr beenden. Wenn sich eine vApp mit den normalen Methoden nicht mehr beenden lässt, können Sie das Beenden erzwingen, um zu verhindern, dass dem Benutzer eine Rechnung zugestellt wird.

Beim erzwungenen Beenden einer vApp verbraucht diese weiterhin Ressourcen in vSphere. Nach dem erzwungenen Beenden einer vApp in vCloud Director müssen Sie im vSphere Client den Status der vApp in vSphere überprüfen und die erforderlichen Maßnahmen ergreifen.

Voraussetzungen

Sie müssen als Systemadministrator bei vCloud Director angemeldet sein.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationen]** .
2. Klicken Sie mit der rechten Maustaste auf den Namen der Organisation und wählen Sie den Befehl **[Öffnen]** .
3. Klicken Sie auf die Registerkarte **[Meine Cloud]** und klicken Sie dann im linken Ausschnitt auf **[vApps]** .
4. Klicken Sie mit der rechten Maustaste auf die ausgeführte vApp und wählen Sie den Befehl **[Beenden erzwingen]** .
5. Klicken Sie auf **[Ja]** .

Fast Provisioning virtueller Maschinen

Fast Provisioning spart Zeit, da verknüpfte Klone für Bereitstellungsvorgänge von virtuellen Maschinen verwendet werden.

Ein verknüpfter Klon ist eine virtuelle Maschine, die dieselbe Basisfestplatte wie das Original verwendet, wobei jedoch eine Kette von Delta-Festplatten erstellt und verwaltet wird, über die Änderungen zwischen dem Original und dem Klon verfolgt werden. Wenn Fast Provisioning deaktiviert ist, resultieren alle Bereitstellungsvorgänge in vollständigen Klonen.

Da ein verknüpfter Klon nicht in einem anderen vCenter-Datencenter oder Datenspeicher als die ursprüngliche virtuelle Maschine vorhanden sein kann, erstellt vCloud Director virtuelle Schattenmaschinen, um die vCenter-Datencenter- und Datenspeicher-übergreifende Erstellung von verknüpften Klonen für virtuelle Maschinen zu unterstützen, die einer vApp-Vorlage zugeordnet sind. Eine virtuelle Schattenmaschine ist eine exakte Kopie der ursprünglichen virtuellen Maschine. Sie wird in dem Datencenter und Datenspeicher erstellt, in dem der verknüpfte Klon erstellt wird. Sie können eine Liste der virtuellen Schattenmaschinen anzeigen, die zu einer virtuellen Vorlagenmaschine gehören. Weitere Informationen erhalten Sie unter „Anzeigen der einer virtuellen Maschine zugeordneten virtuellen Schattenmaschinen“, auf Seite 95.

Fast Provisioning ist standardmäßig auf Organisations-vDCs aktiviert. Fast Provisioning setzt vCenter 5.0 und ESXi 5.0-Hosts voraus. Wenn das Provider-vDC, auf dem das Organisations-vDC basiert, ESX/ESXi 4.x-Hosts enthält, müssen Sie Fast Provisioning deaktivieren. Weitere Informationen erhalten Sie unter „Bearbeiten der Speichereinstellungen von Organisations-vDCs“, auf Seite 54.

Anzeigen der einer virtuellen Maschine zugeordneten virtuellen Schattenmaschinen

Virtuelle Schattenmaschinen unterstützten verknüpfte Klone von virtuellen Maschinen, die vCenter Datencenter- und Datenspeicher-übergreifend vApp-Vorlagen zugeordnet sind.

Eine virtuelle Schattenmaschine ist eine genaue Kopie der ursprünglichen virtuellen Maschine, die vCloud Director auf dem Datencenter und dem Datenspeicher erstellt, auf denen ein verknüpfter Klone erstellt wird. Weitere Informationen erhalten Sie unter „Fast Provisioning virtueller Maschinen“, auf Seite 95.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationen]** .
2. Klicken Sie mit der rechten Maustaste auf den Namen der Organisation und wählen Sie den Befehl **[Öffnen]** .
3. Klicken Sie auf die Registerkarte **[Meine Cloud]** und danach im linken Bereich auf **[VMs]** .
4. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **[Eigenschaften]** .

5 Klicken Sie auf die Registerkarte **[Schatten-VMs]** .

Die Registerkarte wird nur für virtuelle Maschinen angezeigt, denen virtuelle Schattenmaschinen zugeordnet sind.

vCloud Director zeigt eine Liste der virtuellen Schattenmaschinen an, die der virtuellen Maschine zugeordnet sind. Die Liste enthält den Namen jeder virtuellen Schattenmaschine in vCenter, den Datenspeicher, auf dem sich die einzelnen virtuellen Schattenmaschinen befinden, und den vCenter Server, zu dem die virtuelle Schattenmaschine gehört.

Verwalten von Systemadministratoren und Rollen

8

Sie können vCloud Director einzelne Systemadministratoren hinzufügen oder Systemadministratoren als einen Teil der LDAP-Gruppe importieren. Sie können auch Rollen hinzufügen und bearbeiten, über die die Berechtigungen der Benutzer in ihrer Organisation festgelegt werden.

Dieses Kapitel behandelt die folgenden Themen:

- „Hinzufügen eines Systemadministrators“, auf Seite 97
- „Importieren eines Systemadministrators“, auf Seite 98
- „Aktivieren oder Deaktivieren eines Systemadministrators“, auf Seite 98
- „Löschen eines Systemadministrators“, auf Seite 98
- „Bearbeiten des Profils und der Kontaktinformationen des Systemadministrators“, auf Seite 98
- „Versenden einer E-Mail-Benachrichtigung an Benutzer“, auf Seite 99
- „Löschen eines Systemadministrators, der nicht mehr auf das System zugreifen kann“, auf Seite 99
- „Importieren einer LDAP-Gruppe“, auf Seite 99
- „Löschen einer LDAP-Gruppe“, auf Seite 100
- „Ändern einer LDAP-Gruppenbeschreibung“, auf Seite 100
- „Rollen und Rechte“, auf Seite 100
- „Erstellen einer Rolle“, auf Seite 101
- „Kopieren einer Rolle“, auf Seite 101
- „Bearbeiten einer Rolle“, auf Seite 101
- „Löschen einer Rolle“, auf Seite 101

Hinzufügen eines Systemadministrators

Sie können in vCloud Director einen Systemadministrator hinzufügen, indem Sie ein Systemadministratorkonto erstellen. Systemadministratoren verfügen über uneingeschränkten Zugriff auf vCloud Director und alle zugehörigen Organisationen.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Administration]** und klicken Sie dann im linken Bereich auf **[Benutzer]** .

2 Klicken Sie auf **[Neu]** .

3 Geben Sie die Kontendaten für den neuen Benutzer ein und klicken Sie dann auf **[OK]** .

Importieren eines Systemadministrators

Sie können einen LDAP-Benutzer als Systemadministrator importieren, um einen Benutzer mit Systemadministratorrechten hinzuzufügen. Systemadministratoren verfügen über uneingeschränkten Zugriff auf vCloud Director und alle zugehörigen Organisationen.

Voraussetzungen

Überprüfen Sie, ob eine gültige Verbindung zu einem LDAP-Server besteht.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **[Administration]** und klicken Sie dann im linken Bereich auf **[Benutzer]** .
2. Klicken Sie auf **[Von LDAP importieren]** .
3. Geben Sie einen Namen oder den Teil eines Namens in das Textfeld ein und klicken Sie dann auf **[Benutzer suchen]** .
4. Wählen Sie die zu importierenden Benutzer aus und klicken Sie dann auf **[Hinzufügen]** .
5. Klicken Sie auf **[OK]** .

Aktivieren oder Deaktivieren eines Systemadministrators

Sie können das Benutzerkonto eines Systemadministrators deaktivieren, sodass sich dieser Benutzer nicht mehr bei vCloud Director anmelden kann. Wenn Sie einen Systemadministrator löschen möchten, müssen Sie zunächst sein Konto deaktivieren.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **[Administration]** und klicken Sie dann im linken Bereich auf **[Benutzer]** .
2. Klicken Sie mit der rechten Maustaste auf den Namen des Benutzers und wählen Sie den Befehl **[Konto aktivieren]** bzw. **[Konto deaktivieren]** .

Löschen eines Systemadministrators

Sie können einen Systemadministrator aus vCloud Director entfernen, indem Sie sein Konto löschen.

Voraussetzungen

Deaktivieren Sie das Konto des Systemadministrators.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **[Administration]** und klicken Sie dann im linken Bereich auf **[Benutzer]** .
2. Klicken Sie mit der rechten Maustaste auf den Benutzernamen und wählen Sie den Befehl **[Löschen]** .
3. Klicken Sie auf **[Ja]** .

Bearbeiten des Profils und der Kontaktinformationen des Systemadministrators

Sie können das Kennwort und die Kontaktinformationen für ein Systemadministratorkonto ändern.

Sie können ausschließlich die Kontendaten von nicht-LDAP-Benutzern ändern.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Administration]** und klicken Sie dann im linken Bereich auf **[Benutzer]** .

2 Klicken Sie mit der rechten Maustaste auf den Benutzernamen und wählen Sie den Befehl **[Eigenschaften]** .

3 Geben Sie die neuen Daten für das Benutzerkonto ein und klicken Sie dann auf **[OK]** .

Versenden einer E-Mail-Benachrichtigung an Benutzer

Sie können eine E-Mail-Benachrichtigung an alle Benutzer in der gesamten Organisation, an alle Systemadministratoren oder an alle Organisationsadministratoren versenden. Mit einer E-Mail-Benachrichtigung können Sie beispielsweise Benutzer über geplante Systemwartungen in Kenntnis setzen.

Voraussetzungen

Überprüfen Sie, ob eine gültige Verbindung zu einem SMTP-Server besteht.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Administration]** und klicken Sie dann im linken Bereich auf **[Benutzer]** .

2 Klicken Sie auf **[Benachrichtigen]** .

3 Wählen Sie die gewünschten Empfänger aus.

4 Geben Sie den Betreff und den Nachrichtentext ein und klicken Sie auf **[E-Mail senden]** .

Löschen eines Systemadministrators, der nicht mehr auf das System zugreifen kann

Sie können eine Liste der Benutzerkonten anzeigen, die nicht mehr auf das System zugreifen können, weil ihre LDAP-Gruppe aus vCloud Director gelöscht worden ist. Sie können entscheiden, ob die betroffenen Benutzer wieder dem System hinzugefügt werden sollen, und sie anschließend unter **[Gesucht & Gefunden]** löschen.

Informationen zum Hinzufügen von Benutzern, die beim Löschen ihrer LDAP-Gruppe irrtümlich aus dem System entfernt wurden, erhalten Sie unter „Hinzufügen eines Systemadministrators“, auf Seite 97 und „Importieren eines Systemadministrators“, auf Seite 98.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Administration]** und klicken Sie dann im linken Bereich auf **[Gesucht & Gefunden]** .

2 Klicken Sie mit der rechten Maustaste auf den Benutzernamen und wählen Sie den Befehl **[Benutzer löschen]** .

Importieren einer LDAP-Gruppe

Sie können eine LDAP-Gruppe als Systemadministratoren importieren, um eine Gruppe von Benutzern mit Systemadministratorrechten hinzuzufügen. Systemadministratoren verfügen über uneingeschränkten Zugriff auf vCloud Director und alle zugehörigen Organisationen.

Voraussetzungen

Überprüfen Sie, ob eine gültige Verbindung zu einem LDAP-Server besteht.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Administration]** und klicken Sie dann im linken Bereich auf **[Gruppen]** .

2 Klicken Sie auf **[Von LDAP importieren]** .

3 Geben Sie einen Namen oder den Teil eines Namens in das Textfeld ein und klicken Sie dann auf **[Gruppen suchen]** .

4 Wählen Sie die zu importierenden Gruppen aus und klicken Sie dann auf **[Hinzufügen]** .

5 Klicken Sie auf **[OK]** .

Löschen einer LDAP-Gruppe

Sie können eine Gruppe von Systemadministratoren aus vCloud Director entfernen, indem Sie die zugehörige LDAP-Gruppe löschen.

Wenn Sie eine LDAP-Gruppe löschen, werden Benutzer, deren vCloud Director-Konto ausschließlich auf der Grundlage ihrer Mitgliedschaft in dieser Gruppe beruht, isoliert und können sich nicht mehr anmelden. Weitere Informationen erhalten Sie unter „Löschen eines Systemadministrators, der nicht mehr auf das System zugreifen kann“, auf Seite 99.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Administration]** und klicken Sie dann im linken Bereich auf **[Gruppen]** .

2 Klicken Sie mit der rechten Maustaste auf den Gruppennamen und wählen Sie den Befehl **[Löschen]** .

3 Klicken Sie auf **[Ja]** , um den Löschvorgang zu bestätigen.

Ändern einer LDAP-Gruppenbeschreibung

Sie können einer LDAP-Gruppe eine Beschreibung hinzufügen oder ihre Beschreibung ändern, beispielsweise, um mehr Informationen zu der Gruppe anzuzeigen.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Administration]** und klicken Sie dann im linken Bereich auf **[Gruppen]** .

2 Klicken Sie mit der rechten Maustaste auf den Gruppennamen und wählen Sie den Befehl **[Eigenschaften]** .

3 Geben Sie eine Beschreibung für die Gruppe ein und klicken Sie dann auf **[OK]** .

Rollen und Rechte

vCloud Director verwendet Rollen und Rechte, um zu bestimmen, welche Aktionen Benutzer in einer Organisation durchführen dürfen. In vCloud Director sind einige Rollen mit bestimmten Rechten vordefiniert.

System- und Organisationsadministratoren müssen jedem Benutzer und jeder Gruppe eine Rolle zuweisen. Ein Benutzer kann in verschiedenen Organisationen verschiedene Rollen haben. Systemadministratoren können auch Rollen erstellen und und bestehende Rollen bearbeiten.

Weitere Informationen zu den vordefinierten Rollen und den jeweiligen Rechten erhalten Sie unter „Vordefinierte Rollen und ihre Rechte“, auf Seite 123.

Erstellen einer Rolle

Wenn die bestehenden Rollen den Anforderungen nicht mehr genügen, können Sie eine neue Rolle erstellen und ihr die benötigten Berechtigungen zuweisen. Wenn Sie eine Rolle erstellen, ist sie anschließend für alle Organisationen in dem System verfügbar.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Administration]** und klicken Sie dann im linken Bereich auf **[Rollen]** .

2 Klicken Sie auf **[Neu]** .

3 Geben Sie einen Namen und bei Bedarf eine Beschreibung für die Rolle ein.

4 Wählen Sie die Berechtigungen für die Rolle aus und klicken Sie dann auf **[OK]** .

Kopieren einer Rolle

Sie können Rollen anhand bestehender Rollen erstellen, indem Sie eine Rolle kopieren und dann die Berechtigungen anpassen.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Administration]** und klicken Sie dann im linken Bereich auf **[Rollen]** .

2 Klicken Sie mit der rechten Maustaste auf eine Rolle und wählen Sie den Befehl **[Kopieren in]** .

3 Geben Sie einen Namen und bei Bedarf eine Beschreibung für die Rolle ein.

4 Wählen Sie die Berechtigungen für die Rolle aus und klicken Sie dann auf **[OK]** .

Bearbeiten einer Rolle

Sie können den Namen, die Beschreibung und die Berechtigungen einer Rolle bearbeiten.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Administration]** und klicken Sie dann im linken Bereich auf **[Rollen]** .

2 Klicken Sie mit der rechten Maustaste auf eine Rolle und wählen Sie den Befehl **[Eigenschaften]** .

3 Bearbeiten Sie den Namen und bei Bedarf die Beschreibung für die Rolle.

4 Wählen Sie die neuen Berechtigungen für die Rolle aus und klicken Sie dann auf **[OK]** .

Bei Benutzern, die zum Zeitpunkt der Bearbeitung angemeldet sind, werden Änderungen der Rolle erst dann übernommen, wenn der Cache für die aktuelle Sitzung des Benutzers abläuft, oder sich der Benutzer ab- und wieder anmeldet.

Löschen einer Rolle

Sie können eine Rolle aus dem System löschen. Die Rolle des Systemadministrators und Rollen, die aktuell verwendet werden, können nicht gelöscht werden.

Voraussetzungen

Weisen Sie allen Benutzern, denen die zu löschende Rolle zugewiesen ist, eine andere Rolle zu.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Administration]** und klicken Sie dann im linken Bereich auf **[Rollen]** .

2 Klicken Sie mit der rechten Maustaste auf eine Rolle und wählen Sie den Befehl **[Löschen]** .

3 Klicken Sie auf **[Ja]** , um den Löschvorgang zu bestätigen.

Verwalten der Systemeinstellungen 9

vCloud Director-Systemadministratoren können die systemweit geltenden Einstellungen in Zusammenhang mit LDAP, E-Mail-Benachrichtigung und Lizenzierung sowie allgemeine Systemeinstellungen steuern.

Dieses Kapitel behandelt die folgenden Themen:

- „Bearbeiten der allgemeinen Systemeinstellungen“, auf Seite 103
- „Allgemeine Systemeinstellungen“, auf Seite 104
- „Konfigurieren der SMTP-Einstellungen“, auf Seite 105
- „Konfigurieren der Systembenachrichtigungseinstellungen“, auf Seite 106
- „Konfigurieren von blockierenden Aufgaben und Benachrichtigungen“, auf Seite 106
- „Konfigurieren der System-LDAP-Einstellungen“, auf Seite 108
- „Anpassen der Benutzeroberfläche des vCloud Director-Clients“, auf Seite 111
- „Konfigurieren der öffentlichen Web-URL“, auf Seite 113
- „Konfigurieren der Proxy-Adresse der öffentlichen Konsole“, auf Seite 113
- „Konfigurieren der Basis-URL für die öffentliche REST API“, auf Seite 113
- „Konfigurieren der Kontosperrungsrichtlinie“, auf Seite 114

Bearbeiten der allgemeinen Systemeinstellungen

vCloud Director enthält eine Reihe von allgemeinen Systemeinstellungen in Zusammenhang mit den Anmelderichtlinien, Zeitlimits für Sitzungen usw. Die Standardeinstellungen sind in vielen Umgebungen geeignet; Sie können die Einstellungen jedoch bei Bedarf an Ihre Anforderungen anpassen.

Weitere Informationen erhalten Sie unter „Allgemeine Systemeinstellungen“, auf Seite 104.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Administration]** und klicken Sie dann im linken Bereich auf **[Allgemein]** .

2 Bearbeiten Sie die Einstellungen und klicken Sie auf **[Übernehmen]** .

Allgemeine Systemeinstellungen

vCloud Director enthält allgemeine Systemeinstellungen, die Sie an Ihre Anforderungen anpassen können.

Tabelle 9-1. Allgemeine Systemeinstellungen

Name	Kategorie	Beschreibung
Startzeit für Synchronisierung	LDAP-Synchronisierung	Uhrzeit für den Start der LDAP-Synchronisierung
Synchronisierungsintervall	LDAP-Synchronisierung	Anzahl der Stunden zwischen LDAP-Synchronisierungen.
Anmelderichtlinie	Anmelderichtlinie	Wählen Sie eine Anmelderichtlinie aus.
Aufbewahrung des Aktivitätsprotokollverlaufs	Aktivitätsprotokoll	Anzahl der Tage, die der Protokollverlauf aufbewahrt wird, bevor er gelöscht wird. Geben Sie **0**ein, damit Protokolle nie gelöscht werden.
Angezeigter Aktivitätsprotokollverlauf	Aktivitätsprotokoll	Anzahl der Tage im Protokollverlauf, die angezeigt werden. Geben Sie **0** ein, um alle Aktivitäten anzuzeigen.
Debug-Informationen anzeigen	Aktivitätsprotokoll	Aktivieren Sie diese Einstellung, um die Debug-Informationen im vCloud Director-Aufgabenprotokoll anzuzeigen.
Zeitlimit für IP-Adressenfreigabe	Netzwerk	Anzahl an Sekunden, für die freigegebene IP-Adressen gehalten werden, bevor sie erneut für eine Zuweisung verfügbar gemacht werden. Die Standardeinstellung beträgt 2 Stunden (7200 Sekunden), damit alte Einträge aus Client-ARP-Tabellen ablaufen können.
Überschneidungen von externen Netzwerken zulassen	Netzwerk	Aktivieren Sie dieses Kontrollkästchen, um externe Netzwerke hinzuzufügen, die auf demselben Netzwerksegment laufen. Aktivieren Sie diese Einstellung nur dann, wenn Sie zum Isolieren Ihrer externen Netzwerke nicht-VLAN-basierte Methoden (beispielsweise VMware vShield Manager) verwenden.
Standard-Syslog-Servereinstellungen für Netzwerke	Netzwerk	Geben Sie IP-Adressen für bis zu zwei Syslog-Server ein, die von Netzwerken verwendet werden sollen. Diese Einstellung gilt nicht für von Cloud-Zellen verwendete Syslog-Server.
Provider-Gebietsschema	Lokalisierung	Wählen Sie ein Gebietsschema für Provider-Aktivitäten aus. Diese Einstellung wirkt sich auf Protokolleinträge, per E-Mail versendete Warnmeldungen usw. aus.
Zeitlimit für Leerlaufsitzung	Sonstiges	Dauer, für die die vCloud Director-Anwendung aktiv bleibt, wenn der Benutzer keine Eingaben vornimmt.
Maximales Zeitlimit für Sitzung	Sonstiges	Maximale Dauer, für die die vCloud Director-Anwendung aktiv bleibt.
Hostaktualisierungsfrequenz	Sonstiges	Gibt an, wie häufig vCloud Director überprüft, ob auf seine ESX/ESXi-Hosts zugegriffen werden kann.
Zeitlimit für Host-Stillstand	Sonstiges	Wählen Sie aus, wie lange gewartet wird, bis ein Host als im Stillstand gekennzeichnet wird.
Zeitlimit für Übertragungssitzung	Sonstiges	Dauer, bis eine angehaltene oder abgebrochene Uploadaufgabe (z. B. Upload von Medien oder vApp-Vorlagen) mit Fehler beendet wird. Eine Änderung dieser Einstellung hat keine Auswirkungen auf Uploadaufgaben, die aktuell ausgeführt werden.

Tabelle 9-1. Allgemeine Systemeinstellungen (Fortsetzung)

Name	Kategorie	Beschreibung
Aufbewahrung des Chargeback-Ereignisverlaufs	Sonstiges	Anzahl der Tage, die der Chargeback-Ereignisverlauf aufbewahrt wird, bevor er gelöscht wird.
Startzeit der Chargeback-Ereignisbereinigung	Sonstiges	Uhrzeit für den Start der Chargeback-Ereignisverlaufbereinigung.
Standard-vApp-Namen angeben	Sonstiges	Aktivieren Sie dieses Kontrollkästchen, um Standardnamen für vApps zu erzeugen.
Upload-Quarantäne aktivieren mit einem Zeitlimit von __ Sekunden	Sonstiges	Aktivieren Sie dieses Kontrollkästchen und geben Sie eine Zahl ein, die dem Zeitlimit für die Quarantänedauer von hochgeladenen Dateien entspricht. Weitere Informationen zum Arbeiten mit Dateien unter Quarantäne erhalten Sie unter „Überwachen von Dateien unter Quarantäne“, auf Seite 120.
vCenter-Zertifikate überprüfen	Sonstiges	Aktivieren Sie dieses Kontrollkästchen, um vCloud Director den Datenaustausch ausschließlich mit vertrauenswürdigen vCenter Server zu erlauben. Klicken Sie auf **[Durchsuchen]** , navigieren Sie zum JCEKS-Keystore und geben Sie das Kennwort für den Keystore ein.

Konfigurieren der SMTP-Einstellungen

vCloud Director benötigt einen SMTP-Server, um E-Mails zur Benachrichtigung von Benutzern und für Systemwarnungen an Benutzer des Systems zu versenden. Organisationen können die systemweit geltenden SMTP-Einstellungen oder benutzerdefinierte SMTP-Einstellungen verwenden.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Administration]** und klicken Sie dann im linken Bereich auf **[E-Mail]** .

2 Geben Sie den DNS-Hostnamen oder die IP-Adresse des SMTP-Mailservers ein.

3 Geben Sie die Portnummer des SMTP-Servers ein.

4 (Optional) Wenn für den SMTP-Server ein Benutzername erforderlich ist, aktivieren Sie das Kontrollkästchen **[Authentifizierung erforderlich]** und geben Sie einen Benutzernamen und das zugehörige Kennwort für das SMTP-Konto ein.

5 Geben Sie die E-Mail-Adresse ein, die in den vCloud Director-E-Mail-Nachrichten als Absender angezeigt werden soll.

   vCloud Director verwendet die Absender-E-Mail-Adresse, um Warnmeldungen zum Ablauf von Laufzeit- und Speicher-Leases zu versenden.

6 Geben Sie den Text ein, der in den vCloud Director-E-Mail-Nachrichten als Betreff angezeigt werden soll.

7 (Optional) Geben Sie die Empfänger-E-Mail-Adresse ein und klicken Sie dann auf **[SMTP-Einstellungen testen]** .

8 Klicken Sie auf **[Übernehmen]** .

Konfigurieren der Systembenachrichtigungseinstellungen

vCloud Director versendet eine Systemwarnmeldung per E-Mail, wenn wichtige Informationen zu berichten sind. So versendet vCloud Director beispielsweise eine Warnung, wenn auf einem Datenspeicher der Speicherplatz knapp wird. Sie können vCloud Director so konfigurieren, dass Warnmeldungen per E-Mail entweder an alle Systemadministratoren oder an eine festgelegte Liste von E-Mail-Adressen gesendet werden.

Organisationen können die systemweit geltenden Systembenachrichtigungseinstellungen oder benutzerdefinierte Systembenachrichtigungseinstellungen verwenden.

Voraussetzungen

Eine funktionierende Verbindung zu einem SMTP-Server

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Administration]** und klicken Sie dann im linken Bereich auf **[E-Mail]** .

2 Wählen Sie die Empfänger für die Systembenachrichtigung per E-Mail aus und klicken Sie dann auf **[Übernehmen]** .

Konfigurieren von blockierenden Aufgaben und Benachrichtigungen

Blockierende Aufgaben und Benachrichtigungen gestatten einem Systemadministrator, vCloud Director für das Versenden von durch bestimmte Ereignisse ausgelösten AMQP-Nachrichten zu konfigurieren.

Einige dieser Nachrichten sind lediglich Benachrichtigungen über das Stattfinden des Ereignisses. Diese werden Benachrichtigungen genannt. Andere Nachrichten veröffentlichen Informationen an einen festgelegten AMQP-Endpunkt, die anzeigen, dass eine angeforderte Aktion aufgrund einer ausstehenden Aktion durch ein Clientprogramm, das an diesen Endpunkt gebunden ist, blockiert wurde. Diese werden blockierende Aufgaben genannt.

Ein Systemadministrator kann einen systemweit geltenden Satz von blockierenden Aufgaben konfigurieren, die von einer programmgesteuerten Aktion eines AMQP-Clients abhängen.

Konfigurieren eines AMQP Brokers

Sie müssen einen AMQP Broker konfigurieren, wenn vCloud Director durch bestimmte Ereignisse ausgelöste AMQP-Nachrichten versenden soll.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Administration]** und danach im linken Bereich auf **[Blockierende Aufgaben]** .

2 Klicken Sie auf die Registerkarte **[Einstellungen]** .

3 Geben Sie den DNS-Hostnamen oder die IP-Adresse des AMQP-Hosts ein.

Geben Sie den AMQP-Port ein.

Der Standardport ist Port **5672**.

4 Geben Sie den Austauschtyp ein.

5 Geben Sie den vHost ein.

6 Um SSL zu verwenden, aktivieren Sie das SSL-Kontrollkästchen und wählen Sie eine der Zertifikatsoptionen aus.

Option	Aktion
Alle Zertifikate akzeptieren	Aktivieren Sie das Kontrollkästchen.
SSL-Zertifikat	Klicken Sie auf **[Durchsuchen]** und navigieren Sie zu dem gewünschten SSL-Zertifikat.
SSL-Keystore	Klicken Sie auf **[Durchsuchen]** und navigieren Sie zu dem gewünschten SSL-Keystore. Geben Sie das Keystore-Kennwort ein.

7 Geben Sie einen Benutzernamen und ein Kennwort für die Verbindung zum AMQP-Host ein.

8 Klicken Sie zum Testen der Einstellungen auf **[AMQP-Verbindung testen]** .

9 Klicken Sie auf **[Übernehmen]** .

10 (Optional) Aktivieren Sie das Kontrollkästchen **[Benachrichtigungen aktivieren]** oben auf der Seite, um Prüfereignisse für den AMQP-Broker zu veröffentlichen.

Konfigurieren der Einstellungen von blockierenden Aufgaben

Sie können den Statustext, Zeitüberschreitungseinstellungen und Standardaktionen für blockierende Aufgaben festlegen. Die Einstellungen gelten für alle Organisationen in der Installation.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Administration]** und danach im linken Bereich auf **[Blockierende Aufgaben]** .

2 Klicken Sie auf die Registerkarte **[Einstellungen]** .

3 Geben Sie den Text ein, der als Status einer Aufgabe angezeigt wird, deren Ausführung aufgrund einer Erweiterungsverarbeitung blockiert ist.

4 Wählen Sie das Standard-Zeitlimit für Erweiterungen aus.

5 Wählen Sie die Standardaktion bei Zeitlimitüberschreitung aus.

6 Klicken Sie auf **[Übernehmen]** .

Aktivieren von blockierenden Aufgaben

Sie können bestimmte Aufgaben so konfigurieren, dass sie für blockierende Aufgaben aktiviert werden.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Administration]** und danach im linken Bereich auf **[Blockierende Aufgaben]** .

2 Klicken Sie auf die Registerkarte **[Blockierende Aufgaben]** .

3 Wählen Sie die Aufgaben aus, die für blockierende Erweiterungen aktiviert werden sollen.

4 Klicken Sie auf **[Übernehmen]** .

Konfigurieren der System-LDAP-Einstellungen

Sie können vCloud Director so konfigurieren, dass Benutzerkonten unter Verwendung eines LDAP-Servers erstellt und authentifiziert werden. Dies ermöglicht es, bei der Installation einen LDAP-Server zu verwenden und anstelle der manuellen Erstellung der Benutzerkonten die LDAP-Benutzer und -Gruppen zu importieren.

Nach dem Verbinden von vCloud Director mit einem LDAP-Server können Sie Systemadministratoren aus den Gruppen und Benutzern in das LDAP-Verzeichnis importieren. Sie können auch die System-LDAP-Einstellungen verwenden, um die Benutzer und Gruppen in eine Organisation zu importieren, oder Sie können eigene LDAP-Einstellungen für die einzelnen Organisationen festlegen. LDAP-Benutzer können sich erst bei vCloud Director anmelden, nachdem Sie sie in das System oder in eine Organisation importiert haben.

Wenn sich importierte LDAP-Benutzer bei vCloud Director anmelden, überprüft vCloud Director die Anmeldeinformationen anhand des LDAP-Verzeichnisses. Wenn die Anmeldeinformationen angenommen werden, erstellt vCloud Director ein Benutzerkonto und meldet den Benutzer beim System an.

vCloud Director unterstützt hierarchische Domänen für die LDAP-Authentifizierung nicht.

vCloud Director kann die Daten in Ihrem LDAP-Verzeichnis nicht ändern. LDAP-Benutzer und -Gruppen können nur über das LDAP-Verzeichnis selbst hinzugefügt, gelöscht und geändert werden.

Sie können festlegen, wie häufig vCloud Director die Benutzer- und Gruppeninformationen mit dem LDAP-Verzeichnis synchronisiert.

LDAP-Unterstützung

vCloud Director unterstützt verschiedene Kombinationen von Betriebssystem, LDAP-Server und Authentifizierungsmethode.

Tabelle 9-2 zeigt eine Auflistung der von vCloud Director unterstützten Kombinationen an.

Tabelle 9-2. Unterstützte Kombinationen von Betriebssystem, LDAP-Server und Authentifizierungsmethode

Betriebssystem	LDAP-Server	Authentifizierungsmethode
Windows 2003	Active Directory	Einfach
Windows 2003	Active Directory	Einfaches SSL
Windows 2003	Active Directory	Kerberos
Windows 2003	Active Directory	Kerberos-SSL
Windows 2008	Active Directory	Einfach
Windows 7 (2008 R2)	Active Directory	Einfach
Windows 7 (2008 R2)	Active Directory	Einfaches SSL
Windows 7 (2008 R2)	Active Directory	Kerberos
Windows 7 (2008 R2)	Active Directory	Kerberos-SSL
Linux	OpenLDAP	Einfach
Linux	OpenLDAP	Einfaches SSL

Konfigurieren einer LDAP-Verbindung

Sie können eine LDAP-Verbindung konfigurieren, damit vCloud Director und die zugehörigen Organisationen auf die Benutzer und Gruppen auf dem LDAP-Server zugreifen können.

Voraussetzungen

Um Kerberos als Authentifizierungsverfahren verwenden zu können, müssen Sie einen Kerberos-Bereich hinzufügen. Siehe „Hinzufügen eines Kerberos-Bereichs“, auf Seite 110.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Administration]** und klicken Sie dann im linken Bereich auf **[LDAP]** .

2 Geben Sie den Hostnamen oder die IP-Adresse des LDAP-Servers ein.

Verwenden Sie bei der Kerberos-Authentifizierung den vollständig qualifizierten Domänennamen (FQDN).

3 Geben Sie eine Portnummer ein.

Der Standardport für LDAP ist Port 389. Der Standardport für LDAP über SSL (LDAPS) ist Port 636.

4 Geben Sie den Basis-DN (Distinguished Name) ein.

Der Basis-DN ist der Speicherort in dem LDAP-Verzeichnis, mit dem vCloud Director Verbindungen herstellt. VMware empfiehlt, die Verbindung auf der Root-Ebene herzustellen. Geben Sie nur die Domänenkomponenten ein, beispielsweise **`DC=beispiel, DC=com`**.

Wenn Sie eine Verbindung zu einem Knoten in der Baumstruktur herstellen möchten, geben Sie den DN für diesen Knoten ein, beispielsweise **`OU=ServiceDirector, DC=beispiel, DC=com`**. Wenn Sie die Verbindung unter Verwendung eines spezifischen Knotens in dem Verzeichnis herstellen, wird der Verzeichnisbereich, auf den vCloud Director zugreifen kann, entsprechend eingeschränkt.

5 Aktivieren Sie das Kontrollkästchen **[SSL]** , um eine sicher LDAP-Verbindung (LDAPS) zu verwenden, und wählen Sie dann eine der verfügbaren Optionen für Zertifikate.

Option	Aktion
Alle Zertifikate akzeptieren	Aktivieren Sie das Kontrollkästchen.
SSL-Zertifikat	Klicken Sie auf **[Durchsuchen]** und navigieren Sie zu dem gewünschten SSL-Zertifikat.
SSL-Keystore	Klicken Sie auf **[Durchsuchen]** und navigieren Sie zu dem gewünschten SSL-Keystore. Geben Sie das Kennwort ein und bestätigen Sie es.

6 Wählen Sie ein Authentifizierungsverfahren aus.

Option	Beschreibung
Einfach	Bei der einfachen Authentifizierung wird der DN des Benutzers und das Kennwort an den LDAP-Server übermittelt. Wenn Sie LDAP verwenden, wird das LDAP-Kennwort unverschlüsselt über das Netzwerk gesendet.
Kerberos	Kerberos gibt zur Überprüfung der Identität von Benutzern Authentifizierungstickets aus. Wenn Sie die Option **[Kerberos]** wählen, müssen Sie einen Kerberos-Bereich auswählen.

7 Geben Sie einen Benutzernamen und ein Kennwort für die Verbindung zu dem LDAP-Server ein.

Wenn der LDAP-Server so konfiguriert ist, dass Lesezugriff auch ohne Angabe eines Benutzernamens möglich ist, können diese Textfelder frei gelassen werden.

Authentifizierungsmethode	Beschreibung des Benutzernamens
Einfach	Geben Sie den vollständigen LDAP-DN ein.
Kerberos	Geben Sie den vollständigen Namen im Format *benutzer@BEREICH.com* ein.

8 Klicken Sie auf **[Übernehmen]** .

Weiter

Sie können nun dem System und den Organisationen LDAP-Benutzer und -Gruppen hinzufügen, die die LDAP-Einstellungen für das System verwenden.

Hinzufügen eines Kerberos-Bereichs

Um bei LDAP-Verbindungen die Kerberos-Authentifizierung nutzen zu können, benötigt vCloud Director einen Kerberos-Bereich. Sie können einen oder mehrere Bereiche hinzufügen, die anschließend von dem System und den Organisationen genutzt werden können. Das System und die Organisationen können jeweils nur einen Kerberos-Bereich für sich festlegen.

Voraussetzungen

Wenn Sie einen Bereich hinzufügen möchten, müssen Sie zunächst Kerberos als Authentifizierungsmethode auswählen.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Administration]** und klicken Sie dann im linken Bereich auf **[LDAP]** .

2 Klicken Sie auf **[Alle Bereiche bearbeiten]** .

3 (Optional) Wählen Sie auf der Registerkarte **[Bereich]** die Option **[Kerberos-Bereiche mit Kleinschreibung zulassen]** aus, um Kleinbuchstaben in Bereichsnamen zuzulassen.

4 Klicken Sie in der Registerkarte **[Bereich]** auf **[Hinzufügen]** .

5 Geben Sie einen Bereichsnamen und das zugehörige KDC (Key Distribution Center) ein und klicken Sie dann auf **[OK]** .

   Wenn Sie keine Bereiche mit Kleinschreibung zulassen, müssen Bereichsnamen durchgängig in Großbuchstaben geschrieben werden. beispielsweise **`BEREICH`**.

6 Klicken Sie in der Registerkarte **[DNS]** auf **[Hinzufügen]** .

7 Geben Sie einen DNS-Server ein, wählen Sie einen Bereich aus und klicken Sie dann auf **[OK]** .

   Bei der DNS-Angabe können Sie den Punkt (.) als Platzhalterzeichen verwenden. Sie können also beispielsweise **`.beispiel.com`** eingeben.

8 Klicken Sie auf **[Schließen]** und klicken Sie dann auf **[Übernehmen]** .

Weiter

Sie können den hinzugefügten Kerberos-Bereich nun bei der Konfiguration der LDAP-Einstellungen für das System oder für eine Organisation verwenden.

Testen der LDAP-Einstellungen

Nach der Konfigurierung einer LDAP-Verbindung können Sie die Einstellungen testen, um sicherzustellen, dass Benutzer- und Gruppenattribute ordnungsgemäß zugeordnet sind.

Voraussetzungen

Sie müssen eine LDAP-Verbindung konfigurieren, damit Sie sie testen können.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Administration]** und klicken Sie dann im linken Bereich auf **[LDAP]** .

2 Klicken Sie auf **[Testen der LDAP-Einstellungen]** .

3 Geben Sie den Namen eines Benutzers in dem LDAP-Verzeichnis ein und klicken Sie auf **[Test]** .

4 Überprüfen Sie die Zuordnung der Attribute und klicken Sie auf **[OK]** .

Weiter

Basierend auf den Testergebnissen können Sie die LDAP-Benutzer und Gruppenattribute anpassen.

Anpassen der LDAP-Benutzer- und Gruppenattribute

LDAP-Attribute informieren vCloud Director darüber, wie Benutzer- und Gruppeninformationen in dem LDAP-Verzeichnis definiert sind. vCloud Director überführt diese Daten in seine eigene Datenbank. Passen Sie bei Bedarf die Syntax der Benutzer- und Gruppenattribute so an, dass sie denen in dem LDAP-Verzeichnis entsprechen.

Voraussetzungen

Überprüfen Sie, ob eine LDAP-Verbindung besteht.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Administration]** und klicken Sie dann im linken Bereich auf **[LDAP]** .

2 Ändern Sie die Benutzer- und Gruppenattribute und klicken Sie dann auf **[Übernehmen]** .

Synchronisieren von vCloud Director mit dem LDAP-Server

vCloud Director synchronisiert automatisch und in regelmäßigen Abständen die Benutzer- und Gruppeninformationen mit dem LDAP-Server. Sie können die Synchronisierung mit dem LDAP-Server auch jederzeit manuell durchführen.

Für die automatische Synchronisierung können Sie festlegen, wie häufig und zu welcher Zeit die Synchronisierung erfolgen soll. Siehe „Bearbeiten der allgemeinen Systemeinstellungen“, auf Seite 103.

Voraussetzungen

Stellen Sie sicher, dass eine gültige LDAP-Verbindung besteht.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Administration]** und klicken Sie dann im linken Bereich auf **[LDAP]** .

2 Klicken Sie auf **[LDAP synchronisieren]** .

Anpassen der Benutzeroberfläche des vCloud Director-Clients

Sie können das Branding der Benutzeroberfläche des vCloud Director-Clients sowie einige der Links auf dem Anmeldebildschirm der vCloud Director-Startseite anpassen.

Ein Beispiel einer `.css`-Vorlage mit Informationen zu den von vCloud Director für benutzerdefinierte Motive unterstützten Stilen erhalten Sie unter http://kb.vmware.com/kb/1026050.

vCloud Director verwendet im Anmeldebildschirm, in der Kopfzeile und in der Fußzeile sein Standardlogo oder das Logo, das Sie hochladen. Im Anmeldebildschirm wird das Logo in einem Bereich mit einer Mindestabmessung von 48x48 Pixeln bis zu einer Maximalabmessung von 60x150 Pixeln angezeigt. Sie können Logos hochladen, die kleiner als 48x48 Pixel oder größer als 60x150 Pixel sind. vCloud Director skaliert sie in diesem Fall unter Beibehaltung des Seitenverhältnisses so, dass sie in den Anzeigebereich passen. Die hochzuladende Datei darf nicht größer als 16384 Byte sein. In der Kopfzeile und in der Fußzeile wird das Logo entsprechend skaliert, wobei ebenfalls das Seitenverhältnis beibehalten wird.

Die Datei muss im PNG-, JPEG- oder GIF-Format vorliegen.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Administration]** und klicken Sie dann im linken Bereich auf **[Branding]** .

2 Geben Sie einen Unternehmensnamen ein.

Dieser Name wird bei Systemadministratoren in der Titelleiste und für andere Benutzer in der Fußzeile angezeigt.

3 Um ein benutzerdefiniertes Logo auszuwählen, klicken Sie auf **[Durchsuchen]** , wählen Sie eine Datei aus und klicken Sie dann auf **[Öffnen]** .

4 Um ein benutzerdefiniertes Motiv auszuwählen, klicken Sie auf **[Durchsuchen]** , wählen Sie eine `.css`-Datei aus und klicken Sie dann auf **[Öffnen]** .

5 Geben Sie eine URL zu einer Website mit Informationen zu Ihrer vCloud Director-Installation ein.

Beispiel: `http://www.beispiel.com`. Diese Seite wird aufgerufen, wenn Benutzer auf den Unternehmensnamen in der Fußzeile der Client-Benutzeroberfläche klicken.

6 Geben Sie eine URL zu einer Website mit Supportinformationen zu Ihrer vCloud Director-Installation ein.

Diese URL wird aufgerufen, wenn Benutzer auf den Link **[Support]** auf der Registerkarte **[Startseite]** klicken, die für alle vCloud Director-Organisationen verfügbar ist.

7 Geben Sie eine URL zu einer Website ein, über die sich Benutzer für ein vCloud Director-Konto registrieren können.

Dieser Link wird auf der vCloud Director-Anmeldeseite angezeigt.

8 Geben Sie eine URL zu einer Website ein, über die Benutzer ihr Kennwort wiederherstellen lassen können.

Dieser Link wird auf der vCloud Director-Anmeldeseite angezeigt.

9 Klicken Sie auf **[Übernehmen]** .

Zurücksetzen des Systems auf das Standardlogo

Wenn Sie für vCloud Director ein benutzerdefiniertes Logo hochgeladen haben, können Sie das System auf das Standardlogo zurücksetzen.

Voraussetzungen

Stellen Sie sicher, dass Sie ein benutzerdefiniertes Logo hochgeladen haben.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Administration]** und klicken Sie dann im linken Bereich auf **[Branding]** .

2 Wählen Sie die Option **[Systemstandardlogo wiederherstellen]** und klicken Sie auf **[Übernehmen]** .

Zurücksetzen des Systems auf das Standardmotiv

Wenn Sie für vCloud Director ein benutzerdefiniertes Motiv festgelegt haben, können Sie das System jederzeit auf das Standardmotiv zurücksetzen.

Voraussetzungen

Stellen Sie sicher, dass Sie zuvor ein benutzerdefiniertes Motiv angewendet haben.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Administration]** und klicken Sie dann im linken Bereich auf **[Branding]** .

2 Wählen Sie die Option **[Systemstandardmotiv wiederherstellen]** und klicken Sie auf **[Übernehmen]** .

Konfigurieren der öffentlichen Web-URL

Wenn Ihre vCloud Director-Installation mehrere Cloud-Zellen enthält, die hinter einem Lastenausgleichs- oder NAT-Modul ausgeführt werden, oder wenn die Cloud-Zellen über keine öffentlich weiterleitbaren IP-Adressen verfügen, können Sie eine öffentliche Web-URL festlegen.

Während der Ersteinrichtung der einzelnen Cloud-Zellen haben Sie die IP-Adresse eines HTTP-Dienstes angegeben. vCloud Director verwendet standardmäßig diese Adresse, um die Organisations-URL zusammenzustellen, unter der sich die Benutzer der Organisation beim System anmelden. Geben Sie eine öffentliche Web-URL an, wenn Sie eine andere Adresse verwenden möchten.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Administration]** und klicken Sie dann im linken Bereich auf **[Öffentliche Adressen]** .

2 Geben Sie die öffentliche Web-URL ein.

3 Klicken Sie auf **[Übernehmen]** .

Wenn Sie eine Organisation erstellen, enthält die URL der Organisation nun die öffentliche Web-URL anstelle der IP-Adresse des HTTP-Dienstes. vCloud Director passt die anderen Organisations-URLs bestehender Organisationen ebenfalls an.

Konfigurieren der Proxy-Adresse der öffentlichen Konsole

Wenn Ihre vCloud Director-Installation mehrere Cloud-Zellen enthält, die hinter einem Lastenausgleichs- oder NAT-Modul ausgeführt werden, oder wenn die Cloud-Zellen über keine öffentlich weiterleitbaren IP-Adressen verfügen, können Sie für die öffentliche Konsole eine Proxy-Adresse festlegen.

Während der Ersteinrichtung der einzelnen Cloud-Zellen haben Sie die IP-Adresse eines Proxyservers für die Remote-Konsole angegeben. Wenn ein Benutzer versucht, die Konsole einer virtuellen Maschine anzuzeigen, verwendet vCloud Director standardmäßig diese Adresse. Geben Sie eine Proxy-Adresse für die öffentliche Konsole an, wenn Sie eine andere Adresse verwenden möchten.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Administration]** und klicken Sie dann im linken Bereich auf **[Öffentliche Adressen]** .

2 Geben Sie den Hostnamen oder die IP-Adresse für die öffentliche Konsole ein.

   Dies kann die Adresse eines Lastenausgleichsmoduls oder eines anderen Geräts sein, das Datenverkehr an die Proxy-IP der Remote-Konsole weiterleiten kann.

3 Klicken Sie auf **[Übernehmen]** .

Sitzungstickets der Remote-Konsole, die an die IP-Adresse des HTTP-Dienstes gesendet werden, geben die Proxy-Adresse der öffentlichen Konsole zurück.

Konfigurieren der Basis-URL für die öffentliche REST API

Wenn Ihre vCloud Director-Installation mehrere Cloud-Zellen enthält, die hinter einem Lastenausgleichs- oder NAT-Modul ausgeführt werden, oder wenn die Cloud-Zellen über keine öffentlich weiterleitbaren IP-Adressen verfügen, können Sie eine Basis-URL für die öffentliche REST API festlegen.

Während der Ersteinrichtung der einzelnen Cloud-Zellen haben Sie die IP-Adresse eines HTTP-Dienstes angegeben. vCloud Director verwendet bei XML-Antworten aus der REST API und als Uploadziel für den Übertragungsdienst (beim Upload von vApp-Vorlagen und Medien) standardmäßig diese Adresse. Geben Sie eine Basis-URL für die öffentliche REST API an, wenn Sie eine andere Adresse verwenden möchten.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Administration]** und klicken Sie dann im linken Bereich auf **[Öffentliche Adressen]** .

2 Geben Sie den Hostnamen oder die IP-Adresse der Basis-URL für die öffentliche REST API ein.

Dies kann die Adresse eines Lastenausgleichsmoduls oder einer anderen Maschine sein, die Datenverkehr zu der IP des HTTP-Dienstes weiterleiten kann.

3 Klicken Sie auf **[Übernehmen]** .

XML-Antworten von der REST API enthalten nun die Basis-URL und der Übertragungsdienst verwendet die Basis-URL als Uploadziel.

Konfigurieren der Kontosperrungsrichtlinie

Sie können die Kontosperrungsfunktion aktivieren, um zu verhindern, dass sich ein Benutzer nach einer bestimmten Anzahl von Fehlversuchen an der Webkonsole anmeldet. Die Einstellungen, die Sie angeben, gelten standardmäßig für alle Organisationen in der Installation, können jedoch von einem Systemadministrator oder Organisationsadministrator für eine bestimmte Organisation überschrieben werden.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Administration]** und klicken Sie dann im linken Bereich auf **[Kennwortrichtlinie]** .

2 Aktivieren Sie das Kontrollkästchen **[Kontosperrung aktiviert]** oder das Kontrollkästchen **[Systemadministratorkonto kann sperren]** oder beides.

3 Wählen Sie die Anzahl der ungültigen Anmeldungen aus, die akzeptiert werden sollen, bevor ein Konto gesperrt wird.

4 Wählen Sie das Sperrungsintervall aus.

5 Klicken Sie auf **[Übernehmen]** .

Überwachen von vCloud Director 10

Systemadministratoren können abgeschlossene Vorgänge und aktuell bearbeitete Vorgänge überwachen und Informationen zur Nutzung bzw. Auslastung auf der Ebene des Provider-vDCs, des Organisations-vDCs und des Datenspeichers anzeigen.

Dieses Kapitel behandelt die folgenden Themen:

- „Anzeigen von Aufgaben und Ereignissen“, auf Seite 115
- „Überwachen und Verwalten von blockierenden Aufgaben“, auf Seite 117
- „Anzeigen von Informationen zur Nutzung bzw. Auslastung eines Provider-vDCs“, auf Seite 118
- „Anzeigen von Informationen zur Nutzung bzw. Auslastung eines Organisations-vDCs“, auf Seite 118
- „Verwenden des vCloud Director-JMX-Dienstes“, auf Seite 118
- „Anzeigen der vCloud Director-Protokolle“, auf Seite 119
- „vCloud Director und Kostenberichte“, auf Seite 119
- „Überwachen von Dateien unter Quarantäne“, auf Seite 120

Anzeigen von Aufgaben und Ereignissen

Sie können system-- und organisationsbezogene Aufgaben und Ereignisse anzeigen, um vCloud Directory-Aktivitäten zu überwachen und zu überprüfen.

vCloud Director-Aufgaben stellen Vorgänge dar, die sich über einen vergleichsweise langen Zeitraum erstrecken und deren Status sich während des Ablaufs ändert. Beispiel: Normalerweise werden Aufgaben mit dem Status `Wird ausgeführt` gestartet. Wenn die Aufgabe beendet ist, wird ihr Status in `Korrekt ausgeführt` oder in `Fehler` geändert.

vCloud Director-Ereignisse stellen einmalige Geschehnisse dar, die typischerweise in Zusammenhang mit einem zentralen Aspekt eines Vorgangs oder einer bedeutenden Statusänderung für ein vCloud Director-Objekt stehen. So protokolliert vCloud Director beispielsweise ein Ereignis, wenn ein Benutzer die Erstellung eines Organisations-vDC einleitet, und ein anderes, wenn der Vorgang abgeschlossen ist. vCloud Director protokolliert auch ein Ereignis, wenn sich Benutzer anmelden. Darüber hinaus wird festgehalten, ob die Anmeldung erfolgreich durchgeführt wurde.

Anzeigen von aktuellen und abgeschlossenen Systemaufgaben

Zeigen Sie das Systemprotokoll an, um die aktuellen Aufgaben auf Systemebene zu überwachen, nach fehlgeschlagenen Aufgaben zu suchen und Probleme zu behandeln und um Aufgaben nach ihren Besitzern gruppiert anzuzeigen.

Informationen zum Anzeigen der Aufgaben auf Organisationsebene erhalten Sie unter „Anzeigen von aktuellen und abgeschlossenen Organisationsaufgaben“, auf Seite 116.

Je nach den gewählten Einstellungen für vCloud Director enthält das Protokoll auch Debug-Informationen. Siehe „Allgemeine Systemeinstellungen“, auf Seite 104.

Vorgehensweise

1 Melden Sie sich als Systemadministrator beim vCloud Director-System an.

2 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Protokolle]** .

3 Klicken Sie auf die Registerkarte **[Aufgaben]** .

vCloud Director zeigt Informationen zu den einzelnen Aufgaben auf Systemebene an.

4 Doppelklicken Sie auf eine Aufgabe, um Details anzuzeigen.

Anzeigen von aktuellen und abgeschlossenen Organisationsaufgaben

Zeigen Sie das Protokoll für eine Organisation an, um aktuell ausgeführte Aufgaben auf Organisationsebene zu überwachen, nach fehlgeschlagenen Aufgaben zu suchen und Probleme zu behandeln und um Aufgaben nach ihren Besitzern gruppiert anzuzeigen.

Informationen zum Anzeigen der Aufgaben auf Systemebene erhalten Sie unter „Anzeigen von aktuellen und abgeschlossenen Systemaufgaben“, auf Seite 116.

Je nach den gewählten Einstellungen für vCloud Director enthält das Protokoll auch Debug-Informationen. Siehe „Allgemeine Systemeinstellungen“, auf Seite 104.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationen]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen der Organisation und wählen Sie den Befehl **[Öffnen]** .

3 Klicken Sie auf die Registerkarte **[Meine Cloud]** und klicken Sie dann im linken Bereich auf **[Protokolle]** .

4 Klicken Sie auf die Registerkarte **[Aufgaben]** .

vCloud Director zeigt Informationen zu den einzelnen Aufgaben auf Organisationsebene an.

5 Doppelklicken Sie auf eine Aufgabe, um Details anzuzeigen.

Bei den meisten Aufgaben können nur Systemadministratoren die Details anzeigen.

Anzeigen von Systemereignissen

Zeigen Sie das Systemprotokoll an, um Ereignisse auf Systemebene zu überwachen. Sie können nach Ereignissen im Fehlerzustand suchen und Probleme behandeln sowie Ereignisse nach Benutzern gruppiert anzeigen.

Informationen zum Anzeigen der Ereignisse auf der Organisationsebene erhalten Sie unter „Anzeigen von Organisationsereignissen“, auf Seite 117.

Vorgehensweise

1 Melden Sie sich als Systemadministrator beim vCloud Director-System an.

2 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Protokolle]** .

3 Klicken Sie auf die Registerkarte **[Ereignisse]** .

vCloud Director zeigt Informationen zu den einzelnen Ereignissen auf Systemebene an.

4 Doppelklicken Sie auf ein Ereignis, um weitere Informationen anzuzeigen.

Anzeigen von Organisationsereignissen

Sie können das Protokoll einer Organisation anzeigen, um Ereignisse auf Organisationsebene zu überwachen. Sie können nach Ereignissen im Fehlerzustand suchen und Probleme behandeln sowie Ereignisse nach Benutzern gruppiert anzeigen.

Informationen zum Anzeigen der Ereignisse auf Systemebene erhalten Sie unter „Anzeigen von Systemereignissen“, auf Seite 116.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisationen]** .

2 Klicken Sie mit der rechten Maustaste auf den Namen der Organisation und wählen Sie den Befehl **[Öffnen]** .

3 Klicken Sie auf die Registerkarte **[Meine Cloud]** und klicken Sie dann im linken Bereich auf **[Protokolle]** .

4 Klicken Sie auf die Registerkarte **[Ereignisse]** .

vCloud Director zeigt Informationen über die einzelnen Ereignisse auf Organisationsebene an.

5 (Optional) Doppelklicken Sie auf ein Ereignis, um weitere Informationen anzuzeigen.

Nur Systemadministratoren können die Details zu den meisten Ereignissen anzeigen.

Überwachen und Verwalten von blockierenden Aufgaben

Sie können Aufgaben überwachen und verwalten, die sich als Ergebnis der Blockierung in einem ausstehenden Status befinden.

Obwohl Sie blockierende Aufgaben mithilfe der vCloud Director-Webkonsole überwachen und verwalten können, wird jedoch im Allgemeinen erwartet, dass der externe Code unter Verwendung der vCloud-API die AMQP-Benachrichtigungen überwacht und programmgesteuert darauf reagiert.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Blockierende Aufgaben]** .

2 Klicken Sie mit der rechten Maustaste auf eine Aufgabe und wählen Sie eine Aktion aus.

Option	Beschreibung
Fortsetzen	Setzt die Aufgabe fort.
Abbrechen	Bricht die Aufgabe ab und löscht Objekte, die als Teil der Aufgabe erstellt wurden.
///Mit Fehler beenden	Die Aufgabe wird als fehlgeschlagen beendet, ohne dass die als Teil der Aufgabe erstellten Objekte gelöscht werden. Der Status der Aufgabe und ihrer Objekte wechselt zu *Error*.

3 Geben Sie einen Grund ein und klicken Sie auf **[OK]** .

Anzeigen von Informationen zur Nutzung bzw. Auslastung eines Provider-vDCs

Provider-vDCs stellen Organisations-vDCs Rechen-, Arbeitsspeicher- und Speicherressourcen zur Verfügung. Sie können die Provider-vDC-Ressourcen überwachen und bei Bedarf weitere Ressourcen hinzufügen.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Provider-vDCs]** .

2 Klicken Sie auf die Registerkarte **[Überwachen]** .

vCloud Director zeigt Informationen zu CPU-, Arbeitsspeicher und Speicherressourcen für die einzelnen Provider-vDCs an.

Anzeigen von Informationen zur Nutzung bzw. Auslastung eines Organisations-vDCs

Organisations-vDCs stellen Organisationen Rechen-, Arbeitsspeicher- und Speicherressourcen zur Verfügung. Sie können die Organisations-vDC-Ressourcen überwachen und bei Bedarf weitere Ressourcen hinzufügen.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[Organisations-vDCs]** .

2 Klicken Sie auf die Registerkarte **[Überwachen]** .

vCloud Director zeigt Informationen zu CPU-, Arbeitsspeicher und Speicherressourcen für die einzelnen Organisations-vDCs an.

Verwenden des vCloud Director-JMX-Dienstes

vCloud Director-Serverhosts machen über JMX eine Reihe von MBeans öffentlich verfügbar, über die die technische Verwaltung des Servers und der Zugriff auf interne Statistiken erfolgt.

Zugreifen auf den JMX-Dienst unter Verwendung von JConsole

Sie können auf den vCloud Director-JMX-Dienst mit einem beliebigen JMX-Client zugreifen. JConsole ist ein solcher JMX-Client.

Weitere Informationen zu MBeans-Diensten, die über vCloud Director-Umgebungen öffentlich zugänglich gemacht werden, erhalten Sie unter http://kb.vmware.com/kb/1026065.

Voraussetzungen

Der Hostname des vCloud Director-Hosts, zu dem Sie eine Verbindung herstellen möchten, muss von dem DNS sowohl durch Forward- als auch durch Reverse-Lookup des vollständig qualifizierten Domänennamens oder des unqualifizierten Hostnamens aufgelöst werden können.

Vorgehensweise

1 Starten Sie JConsole.

2 Wählen Sie im Menü **[Verbindung]** den Befehl **[Neue Verbindung]** .

3 Klicken Sie auf **[Remote-Verarbeitung]** und geben Sie die URL des JMX-Dienstes ein.

Die URL besteht aus dem Hostnamen oder der IP-Adresse des vCloud Director-Servers, gefolgt von der Portnummer. Beispiel: **`beispiel.com:8999`**. Der Standardport ist Port 8999.

4 Geben Sie den Benutzernamen eines vCloud Director-Systemadministrators und das zugehörige Kennwort ein und klicken Sie dann auf **[Verbinden]** .

5 Klicken Sie auf die Registerkarte **[MBeans]** .

Anzeigen der vCloud Director-Protokolle

vCloud Director stellt für alle Cloud-Zellen im System Protokollinformationen bereit. Sie können die Protokolle anzeigen, um die Zellen zu überwachen und Probleme zu behandeln.

Die Protokolle für die Zellen sind unter `/opt/vmware/cloud-director/logs` gespeichert. Tabelle 10-1 enthält eine Aufstellung der verfügbaren Protokolle.

Tabelle 10-1. vCloud Director-Protokolle

Protokollname	Beschreibung
cell.log	Konsolenausgabe der vCloud Director-Zelle.
vcloud-container-debug.log	Protokollnachrichten der Zelle (Debugging-Ebene).
vcloud-container-info.log	Protokollnachrichten der Zelle (Informationsebene). In diesem Protokoll sind auch Warnungen und Fehler in der Zelle verzeichnet.
vmware-vcd-watchdog.log	Protokollnachrichten des Watchdogs für die Zelle (Informationsebene). In diesem Protokoll finden Sie Informationen zu Systemausfällen der Zelle, zu Neustarts usw.
diagnostics.log	Diagnoseprotokoll für die Zelle. Diese Datei bleibt leer, wenn die Diagnoseprotokollierung in der lokalen Protokollierungskonfiguration deaktiviert ist.
JJJJ_MM_TT.request.log	HTTP-Anforderungsprotokolle im Standard-Apache-Protokollformat

Sie können die Protokolle in beliebigen Texteditoren und -viewern sowie Tools von Drittanbietern anzeigen.

vCloud Director und Kostenberichte

Sie können VMware vCenter Chargeback 1.5 verwenden, um ein Kostenberichtssystem für VMware vCloud Director zu konfigurieren.

Weitere Informationen erhalten Sie im *VMware vCenter Chargeback-Benutzerhandbuch*.

Sie können die Aufbewahrungsdauer des Chargeback-Verlaufs in vCloud Director festlegen. Siehe „Bearbeiten der allgemeinen Systemeinstellungen“, auf Seite 103.

Überwachen von Dateien unter Quarantäne

Mit vCloud Director können von Benutzern in das System hochgeladene Dateien (vApp-Vorlagen und Mediendateien) unter Quarantäne gestellt werden. Sie können die Quarantäne für den Upload aktivieren und die hochgeladenen Dateien unter Verwendung von Tools von Drittanbietern (beispielsweise Virenscannern) weiterverarbeiten, bevor sie von vCloud Director angenommen werden.

Sie können einen beliebigen JMS-Client (Java Message Service) verwenden, der das STOMP-Protokoll zur Überwachung und Beantwortung von Meldungen des vCloud Director-Quarantänedienstes unterstützt.

Wenn eine hochgeladene Datei unter Quarantäne gestellt wird, sendet ein JMS-Broker eine Meldung an eine Anfragewarteschlange in einer Cloud-Zelle. Der Empfänger entscheidet, ob der Upload angenommen oder zurückgewiesen werden soll, indem er eine Meldung in die Antwortwarteschlange einstellt.

Quarantäne für hochgeladene Dateien

Sie können Dateien, die von Benutzern an vCloud Director hochgeladen werden, unter Quarantäne stellen. So können Sie die Dateien verarbeiten (beispielsweise mit einem Virenscanner überprüfen), bevor sie von vCloud Director angenommen werden.

Vorgehensweise

1 Klicken Sie auf die Registerkarte **[Administration]** und klicken Sie dann im linken Bereich auf **[Allgemein]** .

2 Aktivieren Sie das Kontrollkästchen **[Upload-Quarantäne aktivieren]** und geben Sie ein Zeitlimit in Sekunden an.

   Das Zeitlimit gibt die Zeitspanne für die Quarantäne von hochgeladenen Dateien an, nach deren Ablauf die Dateien gelöscht werden.

3 Klicken Sie auf **[Übernehmen]** .

vApp-Vorlagen und Mediendateien, die von Benutzern heraufgeladen werden, stehen erst dann zur Verfügung, wenn sie angenommen worden sind.

Weiter

Richten Sie ein manuelles oder automatisches System ein, um die Nachrichten des Quarantänedienstes entgegenzunehmen, zu verarbeiten und zu beantworten.

Anzeigen von Quarantäneanfragen unter Verwendung von JConsole

Sie können Quarantäneanforderungen unter Verwendung von JConsole anzeigen. Bei der Erstellung der Antwortnachricht benötigen Sie Informationen aus der Anforderungsnachricht.

Voraussetzungen

Die Upload-Quarantäne ist aktiviert.

Vorgehensweise

1 Starten Sie JConsole.

2 Wählen Sie im Menü **[Verbindung]** den Befehl **[Neue Verbindung]** .

3 Klicken Sie auf **[Remote-Verarbeitung]** und geben Sie die URL des JMX-Dienstes ein.

   Die URL besteht aus dem Hostnamen oder der IP-Adresse des vCloud Director-Servers, gefolgt von der Portnummer. Beispiel: **`beispiel.com:8999`**. Der Standardport ist Port 8999.

4 Geben Sie den Benutzernamen eines vCloud Director-Systemadministrators und das zugehörige Kennwort ein und klicken Sie dann auf **[Verbinden]** .

5 Klicken Sie auf die Registerkarte **[MBeans]** und navigieren Sie zu dem Knoten **[org.apache.activemq] > [*uuid*] > [Warteschlange] > [com.vmware.vcloud.queues.transfer.server.QuarantineRequest] > [Betriebe]** .

6 Wählen Sie die Operation `browseMessages()` aus.

7 Kopieren Sie den Text der Nachricht, die Sie beantworten möchten.

Beispiel:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<QuarantineRequestMessage transferSessionId="239d310a-5bce-492d-9e26-eda6b646dc15"
transferSessionFilePath="/opt/vmware/cloud-director/data/transfer/239d310a-5bce-492d-9e26-
eda6b646dc15"
xmlns="http://www.vmware.com/vcloud/v1"/>
```

Weiter

Nehmen Sie die Quarantäneanforderung an oder weisen Sie sie zurück.

Annehmen oder Zurückweisen von Quarantäneanforderungen unter Verwendung von JConsole

Sie können Quarantäneanforderungen unter Verwendung von JConsole annehmen oder zurückweisen. Bei der Erstellung der Antwortnachricht benötigen Sie Informationen aus der Anforderungsnachricht.

Voraussetzungen

Der Text der Anforderungsnachricht liegt Ihnen vor.

Vorgehensweise

1 Kopieren Sie den Text der Anforderungsnachricht in einen Texteditor.

2 Ändern Sie den Namen des XML-Elements in `QuarantineResponseMessage` und fügen Sie dem Element ein neues Attribut hinzu, `response="accept"` bzw. `response="reject"`.

Beispiel:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<QuarantineResponseMessage transferSessionId="239d310a-5bce-492d-9e26-eda6b646dc15"
transferSessionFilePath="/opt/vmware/cloud-director/data/transfer/239d310a-5bce-492d-9e26-
eda6b646dc15"
response="accept"
xmlns="http://www.vmware.com/vcloud/v1"/>
```

3 Starten Sie JConsole.

4 Wählen Sie im Menü **[Verbindung]** den Befehl **[Neue Verbindung]** .

5 Klicken Sie auf **[Remote-Verarbeitung]** und geben Sie die URL des JMX-Dienstes ein.

Die URL besteht aus dem Hostnamen oder der IP-Adresse des vCloud Director-Servers, gefolgt von der Portnummer. Beispiel: **`beispiel.com:8999`**. Der Standardport ist Port 8999.

6 Geben Sie den Benutzernamen eines vCloud Director-Systemadministrators und das zugehörige Kennwort ein und klicken Sie dann auf **[Verbinden]** .

7 Klicken Sie auf die Registerkarte **[MBeans]** und navigieren Sie zu dem Knoten **[org.apache.activemq] > [*uuid*] > [Warteschlange] > [com.vmware.vcloud.queues.transfer.server.QuarantineResponse] > [Betriebe]** .

8 Wählen Sie den Vorgang `sendTextMessage(string, string, string)` aus.

9 Fügen Sie die Antwortnachricht aus dem Texteditor in das erste Feld ein und geben Sie in die anderen Felder den Benutzernamen eines vCloud Director-Systemadministrators und das zugehörige Kennwort ein.

10 Klicken Sie auf **[sendTextMessage]** .

Wenn die Datei angenommen wird, gibt vCloud Director sie aus der Quarantäne frei und schließt den Upload ab. Wenn die Datei zurückgewiesen wird, entfernt vCloud Director die Datei.

11 Rollen und Rechte

vCloud Director verwendet Rollen und die mit ihnen einhergehenden Rechte, um zu bestimmen, welche Benutzer und Gruppen zur Durchführung bestimmter Vorgänge berechtigt sind. Systemadministratoren können Rollen erstellen und bearbeiten. System- und Organisationsadministratoren können Benutzern und Gruppen in einer Organisation Rollen zuweisen.

In vCloud Director sind einige Rollen vordefiniert.

- Systemadministrator
- Organisationsadministrator
- Katalogautor
- vApp-Autor
- vApp-Benutzer
- Nur Konsolenzugriff

Vordefinierte Rollen und ihre Rechte

In vCloud Director sind vordefinierte Rollen integriert. Jeder Rolle ist ein Satz von Standardrechten zugeordnet.

Tabelle 11-1 enthält eine Liste der vordefinierten vCloud Director-Rollen und der Rechte, die den einzelnen Rollen standardmäßig zugeordnet sind. Systemadministratoren können neue Rollen erstellen und bestehende Rollen bearbeiten; lediglich die Rolle „Systemadministrator“ kann nicht geändert werden.

Tabelle 11-1. Standardrechte für vordefinierte Rollen

	Systemadministrator	Organisationsadministrator	Katalogautor	vApp-Autor	vApp-Benutzer	Nur Konsolenzugriff
vApp: vApp erstellen/neu konfigurieren	X	X	X	X		
vApp: vApp löschen	X	X	X	X	X	
vApp: vApp-Eigenschaften bearbeiten	X	X	X	X	X	
vApp: vApp starten/beenden/anhalten/zurücksetzen	X	X	X	X	X	

Tabelle 11-1. Standardrechte für vordefinierte Rollen (Fortsetzung)

	Systemadministrator	Organisationsadministrator	Katalogautor	vApp-Autor	vApp-Benutzer	Nur Konsolenzugriff
vApp: vApp freigeben	X	X	X	X	X	
vApp: vApp kopieren	X	X	X	X	X	
vApp: Zugriff auf die VM-Konsole	X	X	X	X	X	X
vApp: Besitzer ändern	X	X				
vApp: VM-Eigenschaften bearbeiten	X	X	X	X	X	
vApp: VM-Arbeitsspeicher bearbeiten	X	X	X	X		
vApp: CPU der VM bearbeiten	X	X	X	X		
vApp: VM-Netzwerk bearbeiten	X	X	X	X	X	
vApp: VM-Festplatte bearbeiten	X	X	X	X		
vApp: VM-Kennworteinstellungen verwalten	X	X	X	X	X	X
Katalog: Neuen Katalog erstellen/löschen	X	X	X			
Katalog: Katalogeigenschaften bearbeiten	X	X	X			
Katalog: vApp von „Meine Cloud“ hinzufügen	X	X	X	X		
Katalog: Katalog veröffentlichen	X	X	X			
Katalog: Katalog freigeben	X	X	X			
Katalog: Private und freigegebene Kataloge anzeigen	X	X	X	X		
Katalog: Veröffentlichte Kataloge anzeigen	X	X				
Katalog: Besitzer ändern	X	X				

Tabelle 11-1. Standardrechte für vordefinierte Rollen (Fortsetzung)

	Systemadministrator	Organisationsadministrator	Katalogautor	vApp-Autor	vApp-Benutzer	Nur Konsolenzugriff
Katalogobjekt: vApp-Vorlage/Medieneigenschaften bearbeiten	X	X	X			
Katalogobjekt: vApp-Vorlage oder -Medien erstellen/hochladen	X	X	X			
Katalogobjekt: vApp-Vorlage herunterladen	X	X	X			
Katalogobjekt: vApp-Vorlage oder -Medien kopieren/verschieben	X	X	X	X		
Katalogobjekt: vApp-Vorlagen und -Medien anzeigen	X	X	X	X	X	
Katalogobjekt: Zu „Meine Cloud“ hinzufügen	X	X	X	X	X	
Organisation: Eigenschaften der Organisation bearbeiten	X	X				
Organisation: SMTP-Einstellungen bearbeiten	X	X				
Organisation: Kontingent-Richtlinie bearbeiten	X	X				
Organisation: Organisationen anzeigen	X	X				
Organisation: Eigenschaften des Organisationsnetzwerks bearbeiten	X	X				
Organisation: Organisationsnetzwerke anzeigen	X	X				
Organisation: Lease-Richtlinie bearbeiten	X	X				

Tabelle 11-1. Standardrechte für vordefinierte Rollen (Fortsetzung)

	Systemadministrator	Organisationsadministrator	Katalogautor	vApp-Autor	vApp-Benutzer	Nur Konsolenzugriff
Organisation: Kennwortrichtlinie bearbeiten	X	X				
Organisations-vDC: Organisations-vDCs anzeigen	X	X				
Benutzer: Gruppe/Benutzer anzeigen	X	X				
Allgemein: Benachrichtigung senden	X	X				
Allgemein: Administratorsteuerung	X	X				
Allgemein: Administratoransicht	X	X				

Index

A

Aktivitätsprotokoll **116, 117**
Aktualisieren von vCenter Server **81**
allgemeine Systemeinstellungen **103, 104**
AMQP Broker **106**
anmelden **12**
Aufgaben mit Anleitung **12**

B

Basis-URL für öffentliche VCD-REST API **113**
Benachrichtigungen, Informationen **106**
Benutzereinstellungen **14**
blockierende Aufgaben
  Aufgaben konfigurieren **107**
  Informationen **106**
  Konfigurieren von Einstellungen **107**
Branding der Benutzeroberfläche
  auf Systemlogo zurücksetzen **112**
  auf Systemmotiv zurücksetzen **112**

C

Cisco Nexus 1000V **21**
Cloud-Ressourcen **17, 43**
Cloud-Zellen
  beenden **77**
  hinzufügen **77**
  löschen **77**
  neu starten **77**
  starten **77**
  verwalten **77**
  Wartungsmeldung **78**

D

Datenspeicher
  aktivieren und deaktivieren **46, 83**
  entfernen **84**
  Kapazität überwachen **47**
  Warnmeldungen zur Festplattenkapazität **47, 84**
DHCP-Netzwerkdienste **60**

E

E-Mail-Benachrichtigungen **48, 99, 106**
E-Mail-Einstellungen **105**
elastisches vDC **30, 47, 50**
erste Schritte **9**
Erweiterungen
  abgebrochen **117**
  fehlgeschlagen **117**
  fortgesetzt **117**
  Konfigurieren von AMQP **106**
ESX/ESXi-Hosts
  Agent aktualisieren **45, 83**
  aktivieren und deaktivieren **44, 81**
  reparieren **45, 83**
  virtuelle Maschinen verschieben **82**
  vorbereiten und Vorbereitung rückgängig machen **45, 82**
externe Netzwerke
  hinzufügen **19**
  IP-Adressen hinzufügen **55**
  löschen **56**
  Name und Beschreibung **55**
  Spezifikation **55**
Externe Netzwerke, definiert **19**

F

Fast Provisioning **31, 51, 54, 95**
Firewallregeln, Reihenfolge festlegen **62**
freigelegte Objekte **84**

G

Gast-Anpassung, vorbereiten **12, 13**
Gesucht & Gefunden **99**

H

Hinzufügen von vSphere-Ressourcen **15**
hochladen
  Medien **39**
  vApps **38**

I

importieren
  Mediendateien **40**
  vApp-Vorlagen **39**
isolierte Objekte
  löschen **85**
  Löschung erzwingen **85**

J

JMX, Zugriff **118**
JMX-Dienst **118**

K

Kataloge
erstellen **38**
hinzufügen **92**
veröffentlichen **37, 40**
Kataloge veröffentlichen **37, 40**
Katalogveröffentlichung, aktivieren **37**
Kennwort ändern **14**
Kennwortrichtlinie **114**
Kerberos-Bereich **110**
Kontosperrung **114**
Kostenberichte **119**

L

Lastenausgleichsmodul **113**
Laufzeit-Leases **23**
LDAP
Attribute anpassen **111**
konfigurieren **108**
synchronisieren **111**
Unterstützung **108**
Verbindung einrichten **108**
Verbindung testen **110**
LDAP-Gruppen, Beschreibung hinzufügen **100**
Leases, Laufzeit und Speicher **23**
Lizenzierung, vShield **17**

M

MBeans **118**
Medien, hochladen **39**
Microsoft Sysprep **12, 13**
MTU-Wert **22**

N

NAT-Zuordnungsregeln, Reihenfolge festlegen **65**
Netzwerkdienste **60**
Netzwerkkontingent **32, 52**
Netzwerkpools
cloudisolierte Netzwerke hinzufügen **76**
definiert **20**
durch cloudisolierte Netzwerke gestützt **21**
Hinzufügen von VLAN-IDs **76**
löschen **77**
MTU-Wert festlegen **22**
Name und Beschreibung **75**
Portgruppen hinzufügen **76**
portgruppenbasiert **21**
VLAN-basiert **20**
Nexus 1000V **21**

O

öffentliche VCD-URL **113**
Organisationen
aktivieren oder deaktivieren **87**
Aufgaben überwachen **116**
benennen **25**
Benutzer und Gruppen **92**
E-Mail-Einstellungen **27, 90**
Einstellungen bestätigen **28**
Ereignisse überwachen **117**
erstellen **24**
Grenzwerteinstellungen **27, 91**
Kataloge veröffentlichen **26**
Katalogveröffentlichung **90**
Kontingenteinstellungen **27, 91**
LDAP-Optionen **25, 89**
Lease-Einstellungen **27, 91**
lokale Benutzer hinzufügen **26**
löschen **88**
Ressourcen zuweisen **28, 29**
SMTP-Einstellungen **90**
SMTP-Server **27**
umbenennen **88**
vApps **93**
verwalten **87**
Verwalten der Ressourcen **92**
vollständiger Name und Beschreibung **88**
Organisations-vDCs
aktivieren oder deaktivieren **53**
benennen **32, 52**
Beschreibung ändern **53**
Einstellungen bestätigen **32, 52**
erstellen **29, 48, 49**
löschen **53**
Namen ändern **53**
Netzwerkkontingent **32, 52**
Netzwerkpool auswählen **32, 52**
Netzwerkpools **54**
Nutzung bzw. Auslastung überwachen **118**
Organisation auswählen **49**
Provider-vDC auswählen **29, 49**
Speicher zuweisen **31, 51**
Speicherkapazität **54**
Zuweisungsmodelle **30, 50**
Zuweisungsmodelleinstellungen **54**
Organisationsnetzwerke
DHCP konfigurieren **60**
Dienste konfigurieren **60**
DNS-Einstellungen ändern **74**
erstellen **56**
extern/direkt **34, 57**
extern/mit NAT-Routing **34, 58**

externe IP-Adressen konfigurieren **63**
Festlegen der Reihenfolge von Firewallregeln **62**
Firewallregel hinzufügen **61**
Firewalls konfigurieren **61**
hinzufügen **33**
intern **35, 59**
IP-Adressen hinzufügen **73**
IP-Maskierung **63**
IP-Nutzung anzeigen **73**
IP-Übersetzung konfigurieren **64**
löschen **73**
Namen und Beschreibung bearbeiten **74**
NAT konfigurieren **64**
Portweiterleitung konfigurieren **64**
Reihenfolge von NAT-Zuordnungsregeln festlegen **65**
Site-to-Site-VPN aktivieren **66**
statisches Routing aktivieren **69**
statisches Routing hinzufügen **69, 71**
Syslog-Servereinstellungen anwenden **75**
Syslog-Servereinstellungen anzeigen **74**
verbundene vApp-Vorlagen **73**
verbundene vApps **73**
verwalten **56**
VPN-Tunnel erstellen **66–68**
zurücksetzen **72**
OVF-Upload **38**

P

Pay-As-You-Go-Zuweisungsmodell **30, 50**
Protokolle **119**
Provider-vDCs
aktivieren oder deaktivieren **43**
definiert **18**
erstellen **18**
Hinzufügen von Speicherkapazität **46**
löschen **44**
Namen ändern **44**
Nutzung bzw. Auslastung überwachen **118**
Ressourcenpools hinzufügen **47**
verwalten **43**

Q

Quarantänedienst
aktivieren **120**
Anforderungen annehmen **121**
Anforderungen anzeigen **120**
Anforderungen zurückweisen **121**
Übersicht **120**

R

Reservierungspool-Zuweisungsmodell **30, 50**
Ressourcen hinzufügen **15**
Rollen
bearbeiten **101**
erstellen **101**
kopieren **101**
löschen **101**
Rollen und Rechte **123**

S

Schnellstartaufgaben **12**
SMTP-Einstellungen **105**
SMTP-Server **90**
Speicher-Leases **23**
System
Aufgaben überwachen **116**
Rollen und Rechte **100**
Systemadministratoren
aus LDAP **98**
deaktivieren **98**
Konten bearbeiten **98**
Konten erstellen **97**
LDAP-Gruppen **99, 100**
löschen **98**
Systembenachrichtigungseinstellungen **106**
Systemeinstellungen **103**
Systemereignisse **116**

T

Technischer Support, erhalten **7**
Thin Provisioning **31, 51, 54**

U

überwachen, Aufgaben und Ereignisse **115**

V

vApps
Beenden erzwingen **94**
Hinzufügen von virtuellen vSphere-Maschinen **93**
Importieren aus vSphere **93**
sichern **94**
Versetzen in Wartungsmodus **94**
VCD-Proxy-Adresse der öffentlichen Konsole **113**
vCenter Chargeback **119**
vCenter Server
anfügen **15, 16**
deaktivieren **80**
Einstellungen bestätigen **17**
entfernen **80**
erneut verbinden **80**

Upgrade **81**
verbinden **16**
Verbindungseinstellungen **79, 80**
vShield Manager-Einstellungen **81**
vShield-Lizenz zuweisen **17**
vCloud Director – Übersicht **9**
vCloud Director überwachen **115**
verknüpfte Klone **95**
virtuelle Maschinen, Importieren aus vSphere **93**
virtuelle Schattenmaschinen **95**
VPN **66**
vShield, Lizenzierung **17**
vShield for VMware Cloud Director-Lizenz **17**
vShield Manager
Einstellungen **81**
verbinden **16**
vSphere
Datenspeicher **83**
freigelegte Objekte **84**
Mediendateien importieren **40**
Ressourcen **79**
virtuelle Maschinen importieren **39**
vSphere Distributed Switches, MTU-Wert festlegen **22**

W

Webkonsole, anmelden **12**

Z

Zuweisungsmodelle **30, 50**
Zuweisungspool-Zuweisungsmodell **30, 50**